Haaga-Helia
ammattikorkeakoulu Oy

NFC-lähimaksamisen tietoturvariskit mobiililaitteella

Teemu Pasuri

5.11.2017

Haaga-Helia ammattikorkeakoulu Oy

Tiivistelmä

5.11.2017

Tekijä(t)
Teemu Pasuri

Koulutusohjelma
Tietojenkäsittely

Raportin/Opinnäytetyön nimi
NFC-lähimaksamisen tietoturvariskit mobiililaitteella

Sivu- ja liitesivumäärä
41 + 6

Opinnäytetyön nimi englanniksi
NFC mobile close payment vulnerabilities

Opinnäytetyössä tutkitaan tietoturvauhkia, joita syntyy käytettäessä NFC-tekniikkaan pohjautuvia lähimaksusovelluksia mobiililaitteella. Selvityksen kohteena on kuinka turvallista lähimaksaminen mobiililaitteella on, minkälaisia tietoturvauhkia voi ilmetä ja kuinka niiltä voidaan suojautua tai kuinka niitä voidaan ennaltaehkäistä. Tämän tutkimuksen tavoitteena on kertoa kuluttajille, kuinka lähimaksusovelluksia voidaan käyttää turvallisesti mobiililaitteella. Työn tarkoituksena on selvittää kuluttajille kuinka mahdollisia tietoturvahyökkäyksiä ja väärinkäyttöjä voidaan minimoida ja miten niitä voidaan ennaltaehkäistä.

Opinnäytetyössä myös selvitettiin kuluttajien käsitystä ja kokemuksia lähimaksumuotojen turvallisuudesta. Tässä työssä selvitettiin mitkä ovat suurimpia tai todennäköisimpiä tietoturvauhkia lähimaksumuotoja käytettäessä. Kyselytutkimuksella selvitettiin mitkä lähimaksumuodot ovat käytetyimpiä tällä hetkellä. Selvityksen kohteena oli milloin ihmiset ovat lähimaksumuotojen käytön aloittaneet ja onko lähimaksusovellusten tuleminen markkinoille vaikuttanut lähimaksumuotojen käyttömääriin. Tässä työssä selvitettiin kuinka usein ihmiset käyttävät lähimaksumuotoja sekä missä he niitä käyttävät eniten.

Tutkimuksen hypoteeseja ovat lisääntyykö lähimaksupalveluiden käyttö koko ajan. Lähimaksupalveluiden käytön lisääntyessä lisääntyvätkö tietoturvamurrot ja väärinkäytöt. Suhtautuvatko ihmiset lähimaksupalveluihin pääosin positiivisesti, mutta herättävätkö ne ihmisissä myös huolta ja negatiivisia tunteita.

Asiasanat
NFC-teknologia, tietoturva, lähimaksaminen, mobiililaite

Sisällys

1 Johdanto

NFC-ominaisuus löytyy nykyään lähes jokaisesta markkinoilla olevasta mobiililaitteesta kuten älypuhelimista ja tableteista. Tämän lisäksi sitä on hyödynnetty lähimaksuominaisuudella varustetuista pankkikorteissa jo pidemmän aikaa. NFC-teknologia perustuu RFID- eli radiotaajuiseen etätunnistus-tekniikkaan. Tämä tekniikka mahdollistaa tiedon etälukemisen ja -tallentamisen käyttäen tageja eli tunnisteita. NFC-tekniikka mahdollistaa kahden NFC-laitteen välisen langattoman kommunikoinnin muutaman senttimetrin etäisyydellä.

NFC-tekniikkaa hyödynnetään pankkien tarjoamissa mobiili lähimaksusovelluksissa, joita on markkinoilla jo useita kuten: Pivo, Nordea Pay, Aktia Wallet ja MobilePay. Lisäksi Applen vastaava lähimaksusovellus on tulossa Suomen markkinoille todennäköisesti vuonna 2018. Mobiili lähimaksusovellukset mahdollistavat maksamisen esimerkiksi kaupan kassalla näyttämällä älypuhelinta NFC-lukijalla varustettuun maksupäätteeseen. NFC-teknologiaa markkinoidaan voimakkaasti palveluntarjoajien toimesta ja sitä kehittävät useat eri ryhmät kuten alemman tason laitteiston valmistajat, ylemmän tason laitteiston valmistajat, kehittäjät, jälleenmyyjät, yritysasiakkaat ja kuluttajat.

Lähimaksusovellusten yleistyessä tulee ottaa huomioon lähimaksamisen turvallisuus. Teknologia on vielä suhteellisen uusi ja lisätieto aiheesta ei varmasti ole pahitteeksi. Tämän työn tarkoituksena on selvittää kuinka turvallista NFC-lähimaksaminen mobiililaitteella on. Tarkoituksena on selvittää minkälaisia tietoturvauhkia tulee esiin NFC-lähimaksutekniikka käytettäessä ja miten niiltä voidaan suojautua. Tarkoituksena on myös selvittää kuluttajille miten tietoturvariskit voidaan minimoida lähimaksuominaisuutta käytettäessä sekä miten NFC-tekniikkaa ja lähimaksusovelluksia voidaan käyttää mahdollisimman turvallisesti.

Tämän työn teoriaosuudessa käsitellään NFC-tekniikkaa yleisesti. Teoriaosuudessa selvitetään mahdolliset NFC-tekniikan haavoittuvuudet sekä hyökkäys- ja suojausmenetelmät. Teoriaosuuden jälkeen haastatteluosuudessa selvitetään kyselytutkimuksen avulla ihmisten kokemuksia ja mielipiteitä lähimaksamisen turvallisuudesta ja vaarallisuudesta. Kyselytutkimuksen avulla pyritään selvittämään ihmisten perusteluita sille minkä takia he pitävät lähimaksamista vaarallisena ja selvitetään kohtaavatko ne teoriaosuudessa ilmi käyneet tietoturvauhat. Kyselytutkimuksen avulla pyritään selvittämään ihmisten mielipiteitä ja kokemuksia siitä miksi he pitävät lähimaksamista turvallisena. Tutkimuksessa selvitetään mitä

lähimaksumuotoa ihmiset käyttävät eniten. Selvitän minkä pankin sovellus on käytetyin ja onko niiden käyttömäärissä suuria eroja sekä pohdiskelen syitä mistä nämä johtuvat. Selvityksen kohteena on kuinka kauan ihmiset ovat lähimaksuominaisuutta käyttäneet. Tutkimuksessa selvitetään ovatko lähimaksusovellukset kasvattaneet lähimaksumuotojen käyttöä. Tutkimuksessa selvitetään kuinka usein ihmiset käyttävät eri lähimaksumuotoja ja mitkä ovat yleisimpiä paikkoja joissa he sitä käyttävät.

2 Lähimaksaminen ja mobiilimaksamisen eri muodot

Termi mobiilimaksaminen kattaa useita erityyppisiä maksuratkaisuja, jotka suoritetaan mobiililaitteella. Lähimaksaminen on jo ennestään tutumpi suurelle yleisölle NFC-radiotaajuisella etätunnistustekniikalla varustetuista lähimaksukorteista. Suomessa NFC-ominaisuudella varustettuja lähimaksukortteja on jo noin 3 miljoonaa kappaletta ja kymmeniä tuhansia niiden vastaanottamiseen aktivoituja maksupäätteitä. Seuraavaksi käsitellään tarkemmin mitä mobiilimaksamisella ja lähimaksamisella tarkoitetaan ja millä tavoin mobiilimaksamista voidaan jaotella eri luokkiin. (Söderlund 2012; Visa Europe 2016.)

2.1 Lähimaksaminen

Lähimaksamisella tarkoitetaan maksamista, jossa lähilukuominaisuudella varustettu kortti viedään muutaman sentin päähän maksupäätteestä. NFC-tekniikalla maksupääte muodostaa turvatun langattoman yhteyden maksukortissa olevaan siruun radioaaltoja pitkin. Lähimaksuominaisuudella varustetussa kortissa on pieni antenni, joka radioyhteyden avulla siirtää maksuvälineen tiedot nopeasti maksupäätteeseen. (Korttiturvallisuus.fi; Nets.)

2.2 Mobiilimaksaminen

Mobiilimaksamisella tarkoitetaan maksamista, joka tapahtuu mobiililaitteella kuten kännykällä, tabletilla tai älykellolla. Mobiilimaksamisen varhaisimpia muotoja olivat ostoautomaatit, josta tuote ostettiin ja maksettiin puhelinsoitolla. Ensimmäiset kaupalliset mobiilimaksamisen menetelmät esiteltiin Suomessa jo vuonna 1997 Soneran toimesta. Juuri ennen vuosituhannen vaihdetta mobiilimaksupalvelut olivat pääosin kokeiluja ja varsinaiseen kaupalliseen käyttöön niistä pystyttiin ottamaan muun muassa SMS-kertalippu Helsingin kaupungin linja-autoissa. Tekstiviestillä maksaminen sai suosiota Suomessa 2000-luvun alussa, kun television sekä puhelinoperaattoreiden tarjoamat soittoäänet ja pelit tulivat markkinoille. Ainoa 2000-luvun puolenvälin jälkeen laajalti levinnyt mobiilimaksumuoto on perustunut RFID- ja NFC-pohjaisiin teknologioihin. (Kivioja 2007, 11-12; Söderlund 2012.)

2.3 Mobiilipankkipalvelut

Mobiilipankkipalveluilla tarkoitetaan kännykällä suoritettuja peruspankkipalveluita kuten laskujen maksamista tai tilitietojen katsomista. Monella pankilla on oma

mobiilipankkisovellus, jolla pankkiasioinnit voidaan hoitaa matkapuhelimella. Mobiilipankkipalveluilla voidaan hoitaa samoja tehtäviä kuin verkkopankkipalveluilla. Mobiilipankkipalveluilla ei suoriteta maksua kassalla. (Söderlund 2012.)

2.4 Etämaksaminen mobiililaitteella

Etämaksamisessa mobiililaitteella maksajan ja maksunsaajan ei tarvitse olla samassa paikassa maksuhetkellä. Etämaksamista mobiililaitteella on hyödynnetty muun muassa EasyPark-sovelluksessa, jolla voi maksaa auton pysäköintiaikaa Suomessa ja muualla Euroopassa. (Söderlund 2012; EasyPark 2017.)

2.5 NFC-lähimaksaminen mobiililaitteella

NFC-lähimaksamisessa mobiililaitteella maksaja ja maksunsaaja ovat lähietäisyydellä toisistaan. Maksutapahtuman välitys pohjautuu RFID-radiotaajuiseen etätunnistukseen, joka on menetelmä tiedon etälukuun ja -tallentamiseen. OP:n Pivo Wallet oli ensimmäinen NFC lähimaksamista mobiililaitteella hyödyntävä sovellus Suomessa. (Haikala 2016.)

Tämä tutkimus on rajattu nimenomaan NFC-lähimaksamiseen mobiililaitteella eli Söderlundin (2012) mallin mukaiseen kolmanteen luokkaan. Mobiili lähimaksamisella viitataan mobiililaitteella suoritettaviin maksuihin, joissa sekä maksaja että maksunsaaja ovat fyysisesti samassa paikassa. Kontaktiton mobiili lähimaksaminen tarkoittaa mobiilimaksamista, jossa maksutietojen välittyminen perustuu radiotaajuuksilla tapahtuvaan tunnistukseen eli NFC-tekniikkaan.

3 NFC-teknologia

NFC eli Near Field Communication-radiotaajuinen etätunnistustekniikka on uudehko teknologia. NFC-teknologia on myös ekosysteemi eli sen kehitystä tukevat useat eri ryhmät kuten alemman tason laitteiston valmistajat, ylemmän tason laitteiston valmistajat, kehittäjät, jälleenmyyjät, yritysasiakkaat ja kuluttajat. NFC syntyi viime vuosikymmennellä. NFC-teknologia on lyhyen kantaman, korkean taajuuden, matalan tiedonsiirtonopeuden ja langattoman kommunikoinnin teknologia kahden NFC:n sallivan laitteen välillä. Kommunikointi kahden NFC-laitteen välillä tapahtuu 13.56 MHz:n taajuudella, jota käytettiin alkujaan RFID:ssa. NFC on rajoittunut toimimaan erittäin lyhyellä etäisyydellä, vaikka RFID pystyy vastaanottamaan ja siirtämään dataa parin merin päähän. Matkapuhelimien pieni koko rajoittaa matkapuhelimeen sijoitettavan antennin korkeutta. Tällä hetkellä integraatio NFC-teknologiasta mobiilipuhelimiin on harkittu käytännöllisimmäksi ratkaisuksi, koska lähes jokaisella on puhelin mukanaan. (Coskun, Ok & Ozdenizci 2011, 1; Dummies.)

NFC-teknologia mahdollistaa kommunikaation NFC:n sallivan puhelimen ja NFC-lukijan tai NFC-tunnisteen välillä. NFC-tagi on noin postimerkin kokoinen pyöreä tai suorakaiteen muotoinen muistilaite, joka voidaan liimata kohteeseen tai upottaa esimerkiksi rannekkeeseen, kuulokkeisiin tai maksukorttiin. NFC-tagiin voidaan ohjelmoida haluttu toiminto erityisellä NFC-tagien luku- ja kirjoitusohjelmalla. NFC-tagissa on pieni mikrosiru, joka sisältää vähän muistia. Mikrosiruun on kiinnitetty antenni. Antenni mahdollistaa mikrosirun tiedon välittämisen NFC-lukijalle. (Coskun, O & O 2011, 1; Pihkala 2017.)

Potentiaalisia NFC-sovelluksia sekä -palveluita, jotka hyödyntävät NFC-teknologiaa ovat lähimaksaminen mobiililaitteella kuten älypuhelimella tai tabletilla, joukkoliikenteessä käytettävät elektroniset liput, kauppojen kanta-asiakaspalvelut, elektroninen henkilöllisyyden tunnistaminen, turvallisuuspalvelut kuten kulunvalvonta, tiedonsiirto lähes minkä tahansa laitteen välillä kuten digitaalikameran, matkapuhelimen tai mediasoittimen, kohdistettu markkinointi ja terveydenhuollossa esimerkiksi potilaan seuranta. Sen soveltuvuus laajaan kirjoon alueita ja lupaava arvon lisäys mahdollisuuksiin on saanut monet akateemikot, tutkijat, organisaatiot ja kaupalliset yhtiöt kiinnostumaan siitä. (Coskun, O & O 2011, 1; Paganini 2012.)

4 NFC:n turvallisuus ja yksityisyys

Verrattaessa mobiilipuhelinta PC:hen teknisellä tasolla, se eroaa siinä että puhelin on enemmän yksityinen esine ja ihmisten mukana aina. Mobiilipuhelin on tärkeä osa käyttäjien elämää ja yleensä se on fyysisen valvonnan alla. Kuitenkin puhelimemme ovat aina fyysisen hyökkäyksen kohteena kuten varkauden ja teknisten langattomien hyökkäysten kohteena, jotka hyödyntävät Bluetooth- tai Wi-Fi-teknologioita. (Coskun, O & O 2011, 241.)

4.1 Turvallisuus yleisesti

Turvallisuus on suojauksen aste tahallista tai vahingollista väärinkäyttöä tai toimintaa vastaan. Jos hyökkääjä käyttää hyväkseen haavoittuvuutta se voi aiheuttaa vahinkoa järjestelmään. Hyökkääjä voi aiheuttaa vahingollista aktiivisuutta tähtäimessään jokin hyöty. Hyökkääjän tavoitteena voi olla vaikeuttaa hyökätyn järjestelmän normaalia toimintaa, saada järjestelmä toimintakyvyttömäksi tai vuotaa jotain informaatiota. (Coskun, O & O 2011, 241.)

4.2 Miksi turvallisuus on tärkeää?

Käyttäjän käyttäessä palvelua kuten tiedonhallintatyökalua hänen päätarkoituksensa on olla vapaa ongelmista, jotka liittyvät palvelun käyttöön. Hänen seuraava motivaationsa voi olla suorituskyvyn maksimointi.

Palvelun käytön määrään voivat vaikuttaa tekniset puutteet sekä turvallisuusongelmat. Ero turvallisuuden ja teknisten puutteiden välillä on se että turvallisuus huomioi ihmisten toiminnan ja älylaitteet yrittävät aiheuttaa tuhoa. Kun taas tekniset ongelmat eivät ole turvallisuusongelmien aiheuttamia. (Coskun, O & O 2011, 242-243.)

Coskunin, O & O:n (2011, 242-243) mukaan turvallisuudesta tuli tärkeä asia viime vuosikymmenellä seuraavista syistä:

- Hyökkääjän näkökulmasta nykyään on enemmän taloudellisia mahdollisuuksia. Hyökkääjä voi ansaita rahaa haitallisen toiminnan avulla.
- Teknisestä näkökulmasta:

    - Internetin käyttäjämäärät nousevat eksponentiaalisesti; tästä syystä media pahansuoville teoille tulee sopivammaksi. Yksi hyökkääjä voi yrittää samaa hyökkäysmetodia moniin potentiaalisiin uhreihin.
    - On vaikeaa upottaa turvallisuusvaatimuksia uusiin sovelluksiin, koska kehitys maksaa paljon IT-alalla ja uusien sovellusten vaatimukset nousevat. Myöskin lopun sovelluksen suunnitteleminen on paljon helpompaa kuin turvallisuusominaisuuksien upottaminen. Tämä siksi, koska upotetun turvallisuusarkkitehtuurin suunnitteleminen vaatii enemmän aikaa ja rahaa.
- Kehittäjän näkökulmasta potentiaaliset ostajat tapaavat arvostaa toiminnallisuutta paljon enemmän kuin turvallisuutta. Siitä huolimatta että turvallisuusominaisuuksien huomioiminen vaatii asiantuntemusta, käyttäjät yleensä huomioivat vain käyttöliittymän.

Turvallisuus on tärkeä asia myös NFC-ekosysteemissä. Tähän vaikuttaa se että NFC on uudehko ja kasvava teknologia sekä integroitu mobiilipuhelimiin. Jokainen omistaa puhelimen ja ihmiset ovat huolestuneita heihin itseensä liittyvistä asioista. Palveluntarjoajat pyrkivät markkinoimaan NFC:tä voimakkaasti. NFC:llä on potentiaalisesti suuret taloudelliset markkinat, joka on painava syy hyökkääjille. (Coskun, O & O 2011, 243.)

5 Turvallisuusongelmat

NFC-pohjaiset järjestelmät kuten kaikki muutkin tietojärjestelmät ovat hyökkäysten kohteena, jotka uhkaavat järjestelmän turvallisuutta ja käyttäjäyksityisyyttä. Eri NFC käyttötilat hyödyntävät erilaisia kommunikointiprotokollia. NFC-laitteet ovat uniikkeja siitä syystä että ne tukevat kolmea eri käyttötilaa: kirjoittaja/lukija, vertaisverkko ja kortin emulointi. Käytetyin tila älypuhelimissa on vertaisverkko-tila, joka mahdollistaa kahden NFC-laitteen siirtää tietoa keskenään. Vertaisverkkotilassa laitteen lähettäessä tietoa se on aktiivisessa tilassa ja vastaanottaessa passiivisessa tilassa. Kirjoittaja/lukija-tilassa siirretään tietoa myös. Erona vertaisverkkotilaan on se että tässä tilassa esimerkiksi kuulokkeet voidaan parittaa älypuhelimen kanssa lukeakseen tietoa puhelimesta. Kolmas käyttötila on kortin emulointitila. Tässä tilassa NFC-laitetta voidaan käyttää kuten lähimaksuominaisuudella varustettua luottokorttia suorittamaan lähimaksuja kassalla tai esittämään esimerkiksi matkalippu lipun lukijaan julkisessa joukkoliikenteessä. (NFC Forum; Triggs 2017.)

Vertaisverkkotila pohjautuu ISO/IEC 18092 NFC IP-1 langattomaan älykorttistandardiin ja kirjoittaja/lukijatila sekä kortin emulointitila ISO/IEC 14443 langattomaan älykorttistandardiin. ISO/IEC 18092 NFC IP-1-standardi määrittelee vertaisverkkotilan käyttäen induktiivista laitteiden paritusta 13,56 megahertzin keskitaajuudella laitteiden liittämiseen. Se myös määrittelee vertaisverkkotilalle muun muassa toiminnallisuudet, siirtonopeudet ja liitännäiset. ISO/IEC 14443-standardi määrittelee muun muassa kirjoittaja/lukijatilan sekä kortin emulointitilan kommunikaatiossa käytettävät ajastukset, sovellusten komennot ja yhteyden muodostamisen nopeuttamisen. (NFC Forum; International Organization for Standardization.)

Osa tietoturvauhista, palveluista ja mekanismeista ovat samankaltaisia kuten kirjoittaja/lukija- ja kortin emulointitilassa, koska ne pohjautuvat samaan ISO/IEC 14443 langattomaan älykorttistandardiin. Vertaisverkkotilassa sen sijaan osa tietoturvauhista, palveluista ja mekanismeista on erilaisia, koska se pohjautuu ISO/IEC 18092 NFC IP-1 langattomaan älykorttistandardiin. Kirjoittaja/lukija-tila koostuu pääosin uhkista ja palveluista, jotka pohjautuvat RFID-infrastruktuuriin. Vertaisverkko-tila sen sijaan eroaa eroaa edellämainitusta, koska siinä laitteen lähettäessä tietoa se on aktiivisessa tilassa ja vastaanottaessa passiivisessa tilassa. Kortin emulointi-tila koostuu uhkista ja palveluista, jotka ovat samankaltaisia kuin lähimaksuominaisuudella varustetuissa maksukorteissa kuten esimerkiksi salakuuntelu. Kortin emulointi-tila koostuu myös muista

käyttötilaongelmista kuten mahdollisuudesta joutua viestihyökkäyksen uhriksi, jossa hyökkääjä käyttää langatonta tiedonsiirtoa lainaamaan tietoa uhrin tagista ja siirtämällä sitä toiseen tagiin. Tämä tarkoittaa sitä että hyökkääjä lisää viestejä kahden laitteen välillä tapahtuvaan tiedonsiirtoon. Tämä on mahdollista vain jos vastaava laite tarvitsee aikaa ennen kuin lähettää pyynnön, koska hyökkäys voidaan toteuttaa tuona ajanjaksona. (Coskun, O & O 2011, 265, 271.)

Coskunin, O & O:n (2011, 265) mukaan kun NFC-pohjaisia järjestelmiä analysoidaan tietoturvan näkökulmasta järjestelmän komponentit sisältäen kaikki kolme käyttötilaa voidaan listata seuraavalla tavoin:

- Turvallisuusongelmat, jotka liittyvät NFC-tagiin.
- Turvallisuusongelmat, jotka liittyvät NFC-lukijaan.
- Turvallisuusongelmat, jotka liittyvät älykorttiin.
- Turvallisuusongelmat, jotka liittyvät kommunikointiin.
- Turvallisuusongelmat, jotka liittyvät väliohjelmistoon ja backend-järjestelmiin.
- Standardisoidut tietoturvaprotokollat.

Seuraavaksi käsitellään tarkemmin NFC-pohjaisten järjestelmien turvallisuusongelmia.

5.1 NFC-tagin turvallisuusongelmat ja hyökkäysmenetelmät

Lukija/kirjoittaja-tilassa osallisena ovat kaksi NFC-laitetta eli NFC-tagi toisella puolella ja NFC-mobiilipuhelin toisella puolella. Tästä syystä käsiteltäessä NFC-järjestelmän turvallisuutta tulee ottaa huomioon myös NFC-tagin turvallisuus sekä NFC-laitteiden välisen kommunikaation turvallisuus. (Coskun, O & O 2011, 266.)

Seuraavaksi tarkastellaan NFC-tagiin kohdistuvia hyökkäysmenetelmiä, kun tagi on valmiustilassa. Hyökkäykset, jotka tapahtuvat NFC-tagin ja NFC-mobiilipuhelimen kommunikaatiota vastaan käsitellään myöhemmin kappaleessa 5.4.

Coskunin, O & O:n (2011, 266) mukaan yleisimmät hyökkäykset NFC-tagia vastaan voidaan jaotella seuraavasti:

- Tagin kloonaus ja tagin imitointi.
- Tagin sisältö muuttuu.
- Tagin vaihtaminen ja tagin piilottaminen.

Seuraavaksi käsitellään tarkemmin NFC-tagiin kohdistuvia hyökkäyksiä ja puolustuskeinoja niitä vastaan.

5.2 Tagin kloonaus, imitointi ja sisällön muuttaminen

> ”RFID-teknologian näkökulmasta kaikista haastavimmat turvallisuusuhat kaupallisissa RFID-sovelluksissa ovat tagin kloonaus ja tagin imitointi.” (Coskun, O & O 2011, 267.)

Tagin kloonauksella tarkoitetaan RFID-tagin tietojen monistamista tai manipuloimista. Hyökkääjän tavoitteena on saada monistettu tai manipuloitu RFID-tagi samankaltaiseksi kuin alkuperäinen, jotta RFID-sovellus hyväksyy sen sopivana. Yksinkertaisissa passiivisissa RFID-järjestelmissä on mahdotonta erottaa kloonattu tagi aidosta tagista. (Tehranipoor 2012, 14)

Tagin imitointi- tai huijaushyökkäyksessä hyökkääjä naamioi tagin vastaamaan aitoa ja houkuttelee uhrin näyttämään laitteensa tagia vasten. Tämä on mahdollista, jos hyökkääjä on saanut saastutettua tagin haitallisella koodilla. Tagi voi pakottaa käyttäjän suorittamaan haitallisen koodin. Käyttäjän kannalta on ikävää että jotkin puhelinmallit on konfiguroitu suorittamaan NFC-tageilta saatuja komentoja automaattisesti. Tehokkain vastatoimi tämän tyyppistä hyökkäystä vastaan on konfiguroida laite ilmoittamaan ennen kuin se suorittaa mitään NFC:ltä saatuja komentoja. (InfoSec Institute 2013.)

Tagin sisältö pystytään muuttamaan huijaushyökkäyksillä. Huijaushyökkäyksessä tarjotaan käyttäjälle väärää informaatiota, joka vaikuttaa aidolta. Huijaushyökkäykset sisältävät väärennetyn toimialueen nimen, väärän puhelinnumeron tai väärää informaatiota jonkin henkilön, asian tai aktiviteetin tunnistuksesta. Väärän Electronic Product Coden (EPC) levittäminen on huijaushyökkäysesimerkki RFID-järjestelmässä. Huijaushyökkäys voidaan myös naamioida URI:in (Uniform Resource Identifier), URL:iin (Uniform Resource Locator), puhelinnumeroon tai SMS-viestiin. (Coskun, O & O 2011, 267-268.)

Kuviossa 1 on kuvattu esimerkki haitallisesta tagista, jossa alkuperäinen tagi on sisältänyt nimen ”NFCLab” ja osoitteen ”http://www.nfclab.com”. Hyökkääjä on naamioinut haitallisen tagin samalla nimellä ”NFCLab”, jotta uhri ei huomaisin sen olevan väärennetty. Hyökkääjä on piilottanut haitalliseen tagiin eri osoitteen ”http://attacker.com/proxy.cgi/http/www.nfclab.com”. Haitallinen osoite ohjaa oikealle sivulle mutta uhrin tietämättä ajaa samaan aikaan haitallisen skriptin. Näin uhri ei

välttämättä edes tiedä tulleensa hyökkäyksen kohteeksi. Riippuen tagin käyttötavasta hinta, hyllynumero ja mikä tahansa muu data tagilla on mahdollista muuttaa tai manipuloida.

Kuvio 1. Esimerkki haitallisesta tagista (Coskun, O & O 2011)

Palvelunestohyökkäyksellä voidaan häiritä asiakkaan ja palveluntarjoajan välistä suhdetta kuormittamalla palvelua niin paljon että asiakas ei pääse käyttämään palvelua. Pahimmillaan tämä johtaa siihen että asiakas lopettaa palvelun käyttämisen sen ollessa ylikuormitettu. Puolustuskeinona tähän voidaan käyttää tagin suojaamista allekirjoitustekniikoilla kuten salauksella. Allekirjoitus ei kuitenkaan suojaa tagin tietoja kloonaamiselta. (Coskun, O & O 2011, 268.)

5.3 NFC-lukijan turvallisuusongelmat

NFC-lukija on tärkeä NFC-laite, joka pääasiallisesti mahdollistaa kortin emulointitilan sovellusten kuten esimerkiksi lähimaksusovelluksen käytön. Merkittävimmät hyökkäysmetodit NFC-lukijaa vastaan ovat sen varastaminen, tuhoaminen ja imitointi. (Coskun, O & O 2011, 268.)

5.4 NFC-lukijan varastaminen tai tuhoaminen

Kuten RFID-lukijat myös NFC-lukijat voivat joutua tuhoamisen tai varastamisen kohteeksi. NFC-lukija on mahdollista sijoittaa vartioimattomaan paikkaan, jos sitä käytetään esimerkiksi itsepalveluautomaatissa eikä se näin vaadi henkilökunnan fyysistä paikalla oloa. NFC-lukija voi sisältää kriittistä informaatiota, kuten kryptograafisia avaimia. Tämä informaatio voi olla hyökkääjän kohteena. Varastetun NFC-lukijan vaikutus on huomattava, koska sen potentiaalinen manipulointi voi mahdollistaa pahantahtoisten hyökkääjien pääsyn NFC:n salliviin puhelimiin. Varastettu lukija mahdollistaa myös pääsyn backend-järjestelmään, jossa voidaan helpottaa mahdollista tiedon manipulointia. (Coskun, O & O 2011, 268.)

5.5 Imitointi

Kun NFC-yhteys on todentamaton hyökkääjät pystyvät helposti väärentämään oikean lukijan identiteetin saadakseen haltuunsa arkaluonteista informaatiota ja myös muuttamaan tietoja tagissa. Näiden hyökkäysten toteutettavuus riippuu autentikoidun lukijan turvallisuustoimenpiteistä. Esimerkiksi, jos kirjautumistiedot on tallennettu lukijaan niin varastetun lukijan avulla voidaan saada pääsy tarvittaviin kirjautumistietoihin, joilla puolestaan saadaan pääsy RFID-tageihin ja backend-järjestelmiin kuten esimerkiksi dokumenttien hallintaan, tietokantoihin tai kirjanpitoon. (Coskun, O & O 2011, 268.)

5.6 Älykortin turvallisuusongelmat

Älykortteja käytetään yleensä Secure Elementiin (SE) NFC:n sallivissa mobiilipuhelimissa. Secure Element (SE) on yhden sirun suojattu mikro-ohjain, jolla on mahdollista isännöidä turvallisesti sovelluksia sekä niiden luottamuksellista ja kryptograafista dataa. Isännöinti tapahtuu sääntöjen ja turvallisuusvaatimusten mukaisesti, jotka on asetettu pankin, lähimaksusovelluksen ja yrityksen johon maksu suoritetaan toimesta. Yksinkertaisesti kuvattuna Secure Element voidaan luokitella siruksi, joka tarjoaa dynaamisen ympäristön datan tallennukseen, datan prosessointiin ja kommunikaatioon turvallisesti. Nykypäivän älypuhelimissa Secure Element on sulautettu suoraan puhelimen laitteistoon, verkon palveluntarjoajan toimittamaan SIM/UICC-korttiin tai SD-korttiin, joka voidaan asentaa puhelimeen. Älykorttien hyökkäykset jaetaan kahteen eri ryhmään: invasiivisiin hyökkäyksiin jossa fyysisesti poistetaan mikroprosessori tai muokataan sitä ja sivukanavan hyökkäyksiin jossa hyökkääjä analysoi älykortin prosessointia. Molemmat hyökkäystavat on mahdollista toteuttaa sekä kontaktin vaativiin älykortteihin että kontaktittomiin älykortteihin (Coskun, O & O 2011, 269; Marwaha 2014.)

5.7 Invasiivinen hyökkäys

Invasiivinen hyökkäys alkaa sirun kuoren poistamisella. Kun sirun kuori on avattu on mahdollista toteuttaa tunnustelu- tai modifikaatiohyökkäys. Tärkein työkalu invasiivisten hyökkäysten toteuttamiseen on ionianturin omaava työasema, jolla kiinnitetään mikroskooppisia neuloja sirun sisäiseen johdotukseen ja näin pystytään joko lukemaan sisäisiä salattuja tietoja tai vahingoittamaan sirua. Jotta anturi pystyy muodostamaan kontaktin on hyökkääjän poistettava ainakin osa suojakerroksesta. Tämä voidaan toteuttaa fyysisesti materiaali syövyttämällä, poraamalla tai laserleikkurilla. Toinen vaihtoehto sirun toimintalogiikan ymmärtämiseksi on purkaa se käänteisessä järjestyksessä. Ensimmäinen vaihe on luoda kartta uudesta prosessorista eli kuvata sirun pinta. Tämä voidaan toteuttaa käyttämällä optista mikroskooppia, joka on varustettu CCD-

kameralla. CCD-kameralla voidaan tuottaa korkearesoluutioisia valokuvia sirun pinnasta. Se on kamera, joka muuntaa infrapunasäteilyn digitaaliseksi signaaliksi. (Skorobogatov 2001.)

Onnistuakseen hyökkääjän täytyy ymmärtää CMOS-tekniikkaa, jota käytetään integroitujen piirien rakentamiseen esimerkiksi mikroprosessoreissa. Hyökkääjän täytyy ymmärtää myös VLSI-tekniikkaa, joka on prosessi luoda integroitu piiri yhdistämällä tuhansia transistoreja yhdeksi siruksi. Tämän lisäksi hyökkääjän on ymmärrettävä mikrotietokone-arkkitehtuureja. Syvemmät kerrokset voidaan tunnistaa toisesta sarjasta valokuvia vasta, kun metallikerrokset on riisuttu pois kerros kerrallaan. Metallikerrokset saadaan pois syövyttämällä. Hyökkäysten toteuttamiseen voidaan käyttää myös kehittyneempiä työkaluja, kuten keskittyneen ionisäteen (FIB) omaavaa työasemaa. FIB:tä käytetään mikro- ja nano-koneistustyökaluna, jolla muokataan tai valmistetaan materiaaleja mikro- ja nanomittakaavassa. FIB-työasemat yksinkertaistavat syvän metallin ja polysilikoonisten linjojen manuaalista tunnustelua, koska se voi koneistaa pois yhden atomikerroksen ilman että seuraavassa kerroksessa olevat atomit häiriintyvät. FIB-työasemaa voidaan käyttää myös sirun muokkaamiseen luomalla uusia yhteenliittämislinjoja sijoittamalla johtavaa materiaalia yhteyden muodostamiseksi tai sillä voidaan luoda jopa uusia transistoreja. Kaikki invasiiviset hyökkäykset ovat suhteellisen monimutkaisia. Ne vaativat tunteja tai viikkoja erikoislaboratoriossa ja prosessin aikana ne tuhoavat alkuperäisen sirun. Lisäksi invasiiviset hyökkäykset vaativat äärimmäisen ammattitaitoisia kemian, fysiikan ja koneenrakennuksen asiantuntijoita ja korkean budjetin. (Skorobogatov 2001.)

5.8 Sivukanavan hyökkäykset ja niiden ehkäiseminen

Sivukanavan hyökkäyksessä hyökkääjä analysoi älykortin prosessointia ja pyrkii siten etsimään heikkouden, jonka kautta pystyy murtautumaan järjestelmään. Elektroniset piirit ovat luonnostaan vuotavia eli ne tuottavat päästöjä sivutuotteina. Tästä syystä prosessia kutsutaan sivukanavan hyökkäykseksi. Nämä päästöt mahdollistavat hyökkääjän selvittää miten piiri toimii ja mitä tietoja se käsittelee. Tämän tyyppisessä hyökkäyksessä informaatio, jota yleensä hyödynnetään sisältää tietoa ajastuksesta, tietoa virrankäytöstä tai jopa elektromagneettisia kenttiä. Sivukanavan hyökkäysten tehokas hyödyntäminen vaatii syvää tuntemusta sisäisestä järjestelmästä, jossa salausalgoritmeja käytetään. Ajastushyökkäykset toteutetaan tutkimalla kohteen laskelmien vaihteluja. Yksinkertaisissa virran analysointi (SPA)-hyökkäyksissä poimitaan informaatiota pohjautuen virrankäytön variaatioihin. Vaihteleva virta-analyysi (DPA) on erityinen virran analysointihyökkäys, joka perustuu RFID-lukijan ja -tagin kommunikaation ajaksi perustetun instanssin

variaatiomuutoksiin. Tarkemmin sanottuna elektromagneettisiin kenttävariaatioihin. Kun RFID-tagi suorittaa kryptograafista operaatiota sitä voidaan käyttää paljastamaan salausavaimet. (Mitrokotsa, Rieback & Tanenbaum 2010, 83.)

Coskunin, O & O:n (2011, 270) mukaan on olemassa kolme eri vastatoimea sivukanavan hyökkäyksiä vastaan: jatkuva suorittaminen, satunnaiset viivästykset ja satunnaistaminen. Jatkuvassa suorittamisessa algoritmit toteutetaan niin, että samat operaatiot suoritetaan samassa järjestyksessä varmistamatta käytettyä tietoa tai avainarvoja. Tämä estää hyökkääjää suorittamasta ajastus- ja yksinkertaisia sivukanavan-analyysejä.

Satunnaisissa viivästyksissä vaihtelevan sivukanavan-analyysi vaatii samat operaatiot suoritettavaksi katsomatta tietoihin tai avainarvoihin. Funktiot, jotka eivät tee muuta kuin pyörivät loopissa satunnaisen ajan voidaan sisällyttää täytäntöönpanoon aiheuttamaan sen että hyökkääjää vaaditaan synkronoimaan saadut tiedot jälkikäteen. Satunnaistamisessa vaihtelevan sivukanavan analyysi myös vaatii että manipuloitujen tietojen ja havaitun sivukanavan välillä on korrelaatio. Tämä saavutetaan jos hyökkääjä manipuloi dataa niin, että muistissa esitetty arvo naamioidaan satunnaisella arvolla. Tämän jälkeen naamioitu arvo poistetaan algoritmin lopussa tuottaakseen salakielen. (Coskun, O & O 2011, 270.)

5.9 Kommunikaation turvallisuusongelmat ja hyökkäysmenetelmät

Kaikissa NFC-teknologian toimintatiloissa hyödynnetään lyhyen kantaman kommunikaatiota. Hyökkääjät voivat tehokkaan radio-laitteen avulla kommunikoida langattomien älykorttien kanssa useiden metrien päästä. Tämän vuoksi hyökkäykset ja uhat kommunikaation aikana ovat mahdollisia sekä kirjoittaja/lukija-, vertaisverkko- että kortin emulointilassa. Kommunikaation aikana mahdollisia hyökkäyksiä ovat salakuuntelu, datan korruptointi, datan muuttaminen, tietojen syöttö sekä mies välissä-hyökkäys. Näitä hyökkäyksiä käsitellään seuraavaksi tarkemmin. (Coskun, O & O 2011, 270.)

5.10 Salakuuntelu ja puolustautuminen sitä vastaan

Salakuuntelu lukeutuu NFC-teknologian yleisimpiin tietoturvauhkiin. Salakuuntelu tapahtuu, kun kolmas osapuoli sieppaa kahden laitteen välillä lähetetyn signaalin. Hyökkääjän onnistuessa sieppaamaan tiedonsiirto kahden laitteen välillä sillä on ainakin teoriassa mahdollisuus saada haltuunsa henkilökohtaisia tietoja. Näitä tietoja voivat olla esimerkiksi luottokorttitiedot tai muut henkilökohtaiset tiedot. (NearFieldCommunication.org 2017.)

Salakuunteluhyökkäys voidaan toteuttaa molempiin suuntiin eli tagista lukijaan ja lukijasta tagiin. Kommunikaatio kahden laitteen välillä NFC:ssä tapahtuu muutaman senttimetrin lähietäisyydellä. Tärkein kysymys on kuinka lähelle hyökkääjän on päästävä saadakseen siepattua käytettävän RF-signaalin. Toimintatila jossa kommunikaatio tapahtuu vaikuttaa paljon, koska niiden toiminnallisuudet ovat erilaisia. Tämä tarkoittaa sitä generoiko lähettäjä oman RF-kenttänsä vai käyttääkö lähettäjä toisen laitteen generoimaa RF-kenttää. On paljon vaikeampaa salakuunnella passiivista laitetta, joka käyttää aktiivisen laitteen generoimaa RF-kenttää. Tämä johtuu siitä, että aktiivinen laite generoi signaalin korkeammalle taajuudelle kuin passiivinen laite. (Coskun, O & O 2011, 270.)

Dataa, jota siirretään passiivisessa tilassa on merkittävästi vaikeampi salakuunnella kuin aktiivisissa tiloissa siirrettävää dataa. Tämä johtuu siitä että passiivisessa tilassa vain kommunikaation aloittanut laite muodostaa RF-kentän. Tästä johtuen hyökkäyspinta-alaa on vähemmän. Aktiivisessa tilassa molemmat laitteet muodostavat oman kentän. Vain passiivisen tilan käyttäminen ei riitä suurimassa osassa sovelluksista jotka siirtävät arkaluonteista dataa, koska ne vaativat toimiakseen sekä aktiivisen että passiivisen tilan. Ainoa oikea ratkaisu salakuuntelun ehkäisemiseen on perustaa suojattu kanava. Suojattu kanava muodostetaan salaamalla viesti salausavaimella. Salausavain tekee alkuperäisestä viestistä lukukelvottoman muille osapuolille. Näin tieto voidaan siirtää vastaanottajalle ja siirron jälkeen vastaanottaja purkaa sen salauksen purkuavaimella,

jolla lukukelvoton viesti avataan luettavaan muotoon. Tämä mahdollistaa sen että vaihdettu tieto ei paljastu kenellekään muulle kuin tarkoitetulle vastaanottajalle. Vain suojatun kanavan osapuolet voivat muokata lähetettyä tietoa. (Coskun, O & O 2011, 21, 272; NFC.cc 2011.)

5.11 Datan korruptointi ja puolustautuminen sitä vastaan

Tietoturvauhkien määrää lisää myös datan korruptointi. Tämä tapahtuu, kun kolmas osapuoli sieppaa lähetetyn signaalin, muokkaa sitä ja lähettää sen jatkamaan matkaansa. Informaatio, jonka vastaanottava osapuoli saa voi olla korruptoitunut. Korruptoituneella informaatiolla hyökkääjä voi aiheuttaa vastaanottajalle ongelmia tiedon kirjoittamisen, lukemisen, varastoinnin, lähettämisen tai käsittelyn aikana. Informaation ollessa korruptoitunut se aiheuttaa odottamattomia vaikutuksia, kun järjestelmä tai sovellus yrittää käsitellä sitä. Vaikutukset voivat vaihdella pienestä tiedon menetyksestä kokonaiseen järjestelmän kaatumiseen. Hyökkääjä voi olla myös halukas varastamaan informaation. Joissain tapauksissa hyökkääjä yksinkertaisesti vain haluaa estää oikean informaation kulun. Tämä tunnetaan usein palvelunestohyökkäyksenä. (NearFieldCommunication.org 2017.)

NFC-laitteet voivat torjua tämän hyökkäyksen, koska ne pystyvät tarkastamaan RF-kentän tiedonsiirron aikana. NFC-laite pystyy tunnistamaan helposti tämän tyyppisen hyökkäyksen johtuen tiedon korruptointia varten vaaditun virran merkittävän korkeasta määrästä. (Coskun, O & O 2011, 272.)

5.12 Datan muuttaminen ja puolustautuminen sitä vastaan

Datan muuttamisessa hyökkääjä pyrkii järjestämään vastaanottavan laitteen vastaanottamaan tietoa, joka on jollain tavoin manipuloitua. Hyökkääjä muuttaa tietoa muokkaamalla sen binääriarvoa. Hyökkääjän tavoitteena on muuttaa tai poistaa arvokasta informaatiota häiritsemällä kommunikaatiota. Tämän informaation täytyy päällisin puolin olla muokattu näyttämään oikealta, jotta vastaanottaja hyväksyy sen. (Radio-Electronics.com.)

Datan muuttamisen ehkäisemiseksi on kaksi tapaa. Käytettäessä tiedonsiirtoon 106:n Baudin tiedonsiirtonopeutta aktiivisessa tilassa hyökkääjän on mahdotonta muuttaa koko informaatiota, joka siirretään RF-linkin kautta. Baud on lähetysnopeuden yksikkö, joka on yhtä suuri kuin kuinka monta kertaa signaali vaihtaa tilaa sekunnissa. Signaaleille, joissa on vain kaksi mahdollista tilaa yksi Baud vastaa yhtä bittiä sekunnissa. Tämä ei kuitenkaan luo täydellistä suojausta, koska osaa biteistä pystytään muuttamaan myös

106:n Baudin tiedonsiirtonopeutta käytettäessä. Johtuen 106:n Baudin tiedonsiirtonopeudesta aktiivinen tila vaaditaan tiedonsiirtoon molempiin päihin, koska passiivisessa tilassa tietoa ei voi lähettää. Paras vaihtoehto puolustautua datan muuttamista vastaan on käyttää suojattua kanavaa. (Radio-Electronics.com.)

5.13 Tietojen syöttö ja puolustautuminen sitä vastaan

Hyökkääjä voi halutessaan lisätä koodia vaihdettuun dataan. Tämä on mahdollista ainoastaan, jos vastaava laite odottaa erittäin pitkän ajan vastatakseen. Tällöin hyökkääjän on mahdollista lähettää data takaisin lähettäjälle aikaisemmin kuin oikea vastaanottaja. Tietojen syöttö onnistuu, jos syötetty data siirretään ennen kuin alkuperäinen laite aloittaa vastaamisen. Jos molemmat datavirrat menevät päällekkäin data vioittuu. (Coskun, O & O 2011, 271.)

On olemassa kolme vastatoimea tietojen syöttöä varten. Ensimmäinen vaihtoehto on se, että vastaanottaja vastaa viivytyksettä. Tässä tapauksessa hyökkääjä ei voi olla nopeampi kuin oikea vastaanottaja. Hyökkääjä voi olla yhtä nopea kuin oikea laite. Jos kaksi laitetta vastaavat samaan aikaan oikeaa dataa ei vastaanoteta. Toinen mahdollinen vastatoimi on se, että oikea vastaanottaja voi kuunnella kanavaa. Tässä tapauksessa laite voi tunnistaa hyökkääjän, joka pyrkii syöttämään tietoja. Kolmas vaihtoehto on perustaa suojattu kanava kahden laitteen välille. (Coskun, O & O 2011, 272.)

5.14 Mies välissä-hyökkäys ja puolustautuminen sitä vastaan

Mies välissä-hyökkäyksessä kahden laitteen välinen kommunikaatio siepataan kolmannen osapuolen toimesta. Kolmas osapuoli toimii linkkinä mutta käyttää vastaanotettua informaatiota ja mahdollisesti muokkaa sitä päästäkseen haluttuun tavoitteeseen. Tämän täytyy tietenkin tapahtua niin että kaksi oikeaa osapuolta eivät ole tietoisia sieppaajasta. On erittäin vaikeaa suorittaa mies välissä-hyökkäys NFC-linkille. (Radio-Electronics.com.)

Kokonaan minimoidakseen riskin on parasta käyttää aktiivinen-passiivinen-kommunikaatiotilaa. Tällä tavoin on mahdollista havaita ja tunnistaa kaikki ei-toivotut kolmannet osapuolet. (Radio-Electronics.com.)

5.15 Väliohjelmiston ja backend-järjestelmän turvallisuus

NFC-pohjainen järjestelmä sisältää NFC-lukijat, NFC-puhelimet ja NFC-tagit. Tästä huolimatta täydellinen NFC-järjestelmä sisältää palvelimet datan tallennukseen ja käsittelyyn kuten pankkipalvelimet, luottokorttiväliohjelmiston, autentikointi-osajärjestelmät

ja niin edelleen. Näin ollen NFC-järjestelmän turvallisuus ei ole täydellinen ellei koko järjestelmän kaikki komponentit ole turvattu. Väliohjelmiston ja backend-järjestelmän täytyy olla turvattu. Tietokannat voivat olla erittäin arkaluonteisia, jos ne sisältävät arvokasta informaatiota kuten luottokorttinumeroita, henkilötunnuksia tai salasanoja. Yritykset voivat jopa menettää asiakkaiden luottamuksen elleivät ne ehkäise vahinkoja tai korjaa niitä nopeasti. On raportoitu paljon yrityksistä, jotka ovat kärsineet suurista vastoinkäymisistä menettämällä asiakkaita johtuen IT:hen liittyvistä vioista. Esimerkiksi Iso-Britannialainen telekommunikaatioyritys TalkTalk myönsi menettäneensä 60 miljoonaa puntaa ja 101 000 asiakasta tietomurron jälkeen. Tietomurto tapahtui lokakuussa 2015 jolloin 156 000:n ihmisen yksityistiedot päätyivät hyökkääjien käsiin. (Coskun, O & O 2011, 272; Hall 2016.)

5.16 Standardisoidut NFC-turvallisuusprotokollat

Standardeja julkaiseva yhdistys ECMA International on julkaissut viisi NFC-standardia, joiden tarkoituksena on varmistaa NFC-kommunikaation laitteiden välisen tiedonsiirron luottamuksellisuus, eheys ja luotettavuus. Nämä standardit ovat ECMA-385, ECMA-386, ECMA-409, ECMA-410 ja ECMA-411. Yhteistä näillä standardeilla on sovellusriippumaton ja turvallinen kuljetuskerros, joka suojaa NFC-laitteiden kommunikaatiota. Nämä standardit pystyvät tehokkaasti käsittelemään tyypillisiä turvallisuusuhkia, kuten väärentäminen, tiedon tuhoutuminen, peukalointi ja mies-välissä-hyökkäys. Standardit ECMA-409, ECMA-410 ja ECMA-411 julkaistiin standardien ECMA-385 ja ECMA-386 jälkeen NFC-SEC-standardiarkkitehtuuriin. (NFC World 2015.)

6 Tunnettuja Suomessa toimivia NFC-mobiilimaksupalveluita ja palveluntarjoajia

Seuraavaksi käsitellään tunnetuimpia Suomessa toimivia NFC-mobiilimaksupalveluita ja palveluntarjoajia. Käsittelyssä ovat neljän tunnetun eri pankin sovellukset: Pivo, Nordea Pay, Aktia Wallet ja MobilePay. Vertailussa pyritään tuomaan esiin eri sovellusten mahdollisia eroavaisuuksia.

6.1 Pivo

Osuuspankin sovellus Pivo otti käyttöön lähimaksut 6.4.2016. Lähimaksuominaisuutta oli mahdollista beetatestata jo vuodesta 2015 alkaen. Itse sovellus sai alkunsa Oulussa vuonna 2012. Pivo on rahansiirto- ja maksupalvelu, jolla voi lähimaksaa kaupan kassalla ja siirtää rahaa toiselle käyttäjälle. Pivon käyttö on maksutonta. OP:n asiakkaat voivat seurata sovelluksella myös rahan kulutustaan. Tällä hetkellä Pivon lähimaksuominaisuus toimii vain OP:n asiakkaille. Pivon lähimaksuominaisuus toimii tällä hetkellä vain älypuhelimissa, joissa on Android-käyttöjärjestelmä. (Lainiala 2016; Pivo.)

6.2 Nordea Pay

Nordea julkaisi sovelluksensa Nordea Pay:n beetatestikäyttöön 3.5.2016. Nordea Pay on maksusovellus, jolla voi lähimaksaa kaupan kassalla, maksaa internet ostokset Masterpassin avulla ja seurata rahankulutusta. Nordea Pay:n käyttöönotto edellyttää Nordean korttia, tunnuslukusovellusta ja Android tai iOS-käyttöjärjestelmää. Lähimaksutoiminto on mahdollinen vain Android-puhelimella. (Haikala 2016; Nordea.)

6.3 Aktia Wallet

Aktia toi markkinoille Aktia Walletin 27.10.2016. Elisa Lompakko– ja Aktian korttisovellus yhdistyivät ja näin syntyi Aktia Wallet. Aktia Wallet on maksusovellus, jolla voi lähimaksaa kaupan kassalla, verkkokaupoissa ja siirtää rahaa toiselle käyttäjälle. Aktia Walletin lähimaksuominaisuus eroaa muista sovelluksista sillä, että lähimaksu suoritetaan lähimaksutarran avulla. Yksi lähimaksutarra maksaa 4,90 € / kpl ja se toimitetaan seitsemän päivän kuluessa tilauksesta. Aktia Walletilla voi seurata Aktian maksukorttien tapahtumia ja asetuksia. Eroavaisuutena muihin sovelluksiin voidaan mainita maarajoitus. Aktia Walletin avulla voi rajata missä päin maailmaa omaa korttia voidaan käyttää ja tällä voidaan estää väärinkäyttöjä. (Aktia; Osakesijoittaja.fi 2016.)

6.4 MobilePay

Danske Bankin MobilePay otti mobiili lähimaksamisen käyttöön ensimmäisen kerran vuoden 2016 kesän festivaaleilla. Tätä ennen sovellusta käytettiin pääasiassa yksilöiden väliseen rahansiirtoon. MobilePay:lla on mahdollista lähimaksaa kassoilla, siirtää rahaa toiselle käyttäjälle ja maksaa verkkokaupoissa. Lähimaksu onnistuu vain tietyissä liikkeissä. Myyjän täytyy olla MobilePay Point of Sale-piste. MobilePay:hin voi rekisteröidä minkä tahansa suomalaisen pankin kortin ja tilin. MobilePay toimii Android ja iOS-käyttöjärjestelmillä. MobilePay:n käyttö on maksutonta. (Haikala 2016; MobilePay.)

7 Tutkimus lähimaksupalveluiden käytöstä

Tämän opinnäytetyön tarkoituksena on selvittää kyselytutkimuksen avulla ihmisten suhtautumista ja kokemuksia lähimaksupalveluiden turvallisuudesta. Tutkimuksen tavoitteena on selvittää myös mitä lähimaksupalveluita ihmiset käyttävät, milloin he ovat käytön aloittaneet, kuinka usein he käyttävät lähimaksupalveluita sekä missä ihmiset lähimaksupalveluita käyttävät.

Tutkimuksen hypoteesit:

- Lähimaksupalveluiden käyttö lisääntyy koko ajan.
- Lähimaksupalveluiden käytön lisääntyessä tietoturvamurrot ja väärinkäytöt lisääntyvät.
- Ihmiset suhtautuvat lähimaksupalveluihin pääosin positiivisesti, mutta ne herättävät ihmisissä myös huolta ja negatiivisia tunteita.

7.1 Tutkimusmenetelmät

Tiedonkeruutavaksi valittiin kyselytutkimus, joka toteutettiin Kyselynetti.com-palvelun avulla. Muita vaihtoehtoja, joilla kyselytutkimus olisi voitu järjestää olivat Google Forms ja Surveymonkey.com. Kyselynetti.com-palvelu sopi tarkoitukseen parhaiten, koska siinä oli ominaisuudet joilla tekemäni kysymykset oli mahdollista toteuttaa sekä selkein käyttöliittymä. Tästä syystä se valittiin. Kyselyyn vastattiin anonyymisti eikä se vaatinut minkäänlaista rekisteröitymistä. Kyselyä jaettiin sosiaalisessa mediassa Facebookissa sekä Whatsapp-pikaviestintäsovelluksessa. Kysely valittiin tiedonkeruutavaksi, jotta saataisiin useita ja monipuolisia vastauksia. Lisäksi kyselyn pohjalta on helppo rakentaa tutkimusdataa kuvaavia kaavioita.

Kyselyn kohdeyleisö oli laaja. Käytännössä kyselyn vastaamiseen riitti, että pystyi muodostamaan itsenäisen mielipiteen lähimaksupalveluista. Kysymykset pyrittiin muotoilemaan mahdollisimman ymmärrettävästi, jotta niihin myös osattaisiin yksiselitteisesti vastata. Kyselyn kysymyksien tarkoitus oli saada vastauksia tutkimuskysymyksiin sekä selvittämään tukevatko tulokset hypoteeseja. Kysely koostui yksi- ja monivalintakysymyksistä sekä vapaamuotoisista vastauksista. Vapaamuotoisia vastauksia käytettiin, jotta vastaajilta saataisiin mahdollisimman paljon perusteltuja vastauksia.

8 Tutkimustulokset

Kysely avattiin perjantaina 11.8. iltapäivällä saateviestin kanssa ja kysely suljettiin torstaina 17.8. puolen päivän aikaan. Aluksi kysely jaettiin julkisena päivityksenä Facebookissa kavereilleni, jotka ovat pääosin iältään noin 20-30-vuotiaita. Tämän jälkeen kysely levisi vanhempieni toimesta myös heidän kollegoilleen ja näin ollen saimme lisää vastauksia noin 50-vuotiailta. Kaiken kaikkiaan kyselyyn vastasi 75 osallistujaa. Kyselyssä oli kysymyksiä yhteensä seitsemän kappaletta, joista kolmeen oli pakko vastata. Pakollisten kysymyksien perässä on *-merkki. Turvallisuuteen liittyvät kysymykset aseteltiin ensimmäisiksi, jotta saisimme mahdollisimman paljon vastauksia myös ihmisiltä, jotka eivät ole lähimaksupalveluita käyttäneet.

Kyselyn kysymykset:

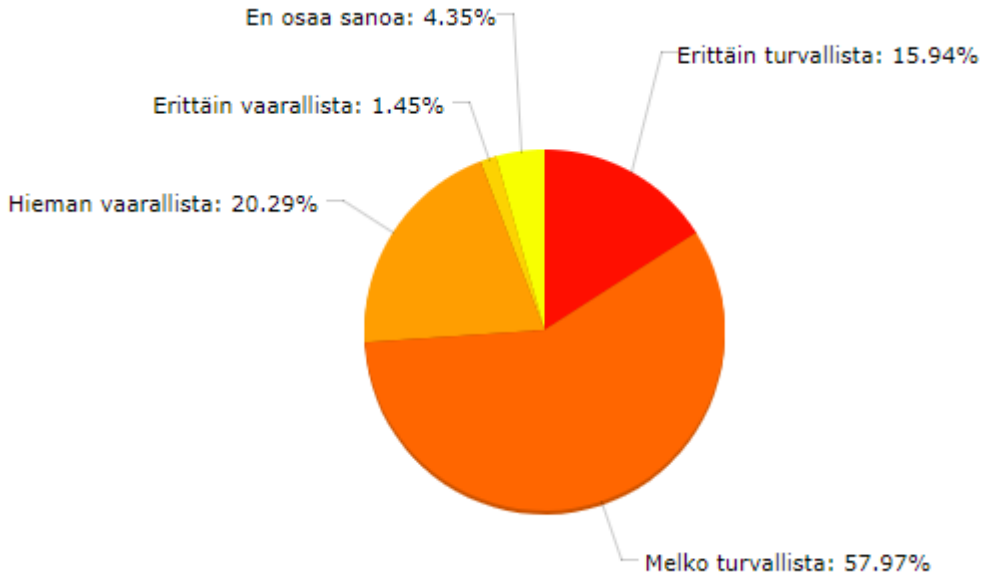
1. Kuinka turvallista lähimaksaminen mielestäsi on?
2. Minkä takia pidät lähimaksamista vaarallisena?
3. Minkä takia pidät lähimaksamista turvallisena?
4. Mitä lähimaksumuotoja käytät? *
5. Kuinka kauan olet käyttänyt lähimaksuominaisuutta? *
6. Kuinka usein käytät lähimaksuominaisuutta?
7. Missä käytät lähimaksuominaisuutta? *

8.1 Lähimaksamisen turvallisuus

Ensimmäisessä kysymyksessä haettiin vastaajien mielipidettä kuinka turvallista lähimaksaminen heidän mielestään on. Kysymyksellä pyrittiin selvittämään lähimaksuominaisuutta käyttäneiden vastaajien kokemuksia siitä onko lähimaksaminen heidän mielestään turvallista vai turvatonta. Vastausvaihtoehdoiksi annettiin erittäin turvallista, melko turvallista, hieman vaarallista, erittäin vaarallista ja en osaa sanoa. Kysymykseen saatiin 69 vastausta. Kysymyksessä ohjattiin vastaajat, jotka eivät olleet lähimaksumuotoja käyttäneet siirtymään suoraan kysymykseen neljä.

Kuviosta 2 ilmenee että vastaajista selkeä enemmistö (58 %) pitää lähimaksamista melko turvallisena. 20,3 % vastaajista pitää lähimaksamista hieman vaarallisena. Erittäin turvallisena lähimaksamista pitää 15,9 % vastaajista. Kolme vastaajaa (4,3 %) ei osannut sanoa kuinka turvallista lähimaksaminen heidän mielestään on. Yksi vastaaja (1,4 %) piti lähimaksamista erittäin vaarallisena. Tämän kysymyksen tulokset tukevat hypoteesia jonka mukaan ihmiset suhtautuvat lähimaksupalveluihin pääosin positiivisesti, mutta ne

herättävät ihmisissä myös huolta ja negatiivisia tunteita. Tutkimuksen toinen hypoteesi oli lähimaksupalveluiden käytön lisääntyessä tietoturvamurrot ja väärinkäytöt lisääntyvät. Tutkimuksen tulokset eivät näytä tukevan tätä olettamusta, koska jos vastaajat olisivat kokeneet henkilökohtaisesti tietoturvamurtoja tai väärinkäyttöjä niin se varmasti näkyisi suurempina vastausmäärinä erittäin vaarallista-kohdassa.



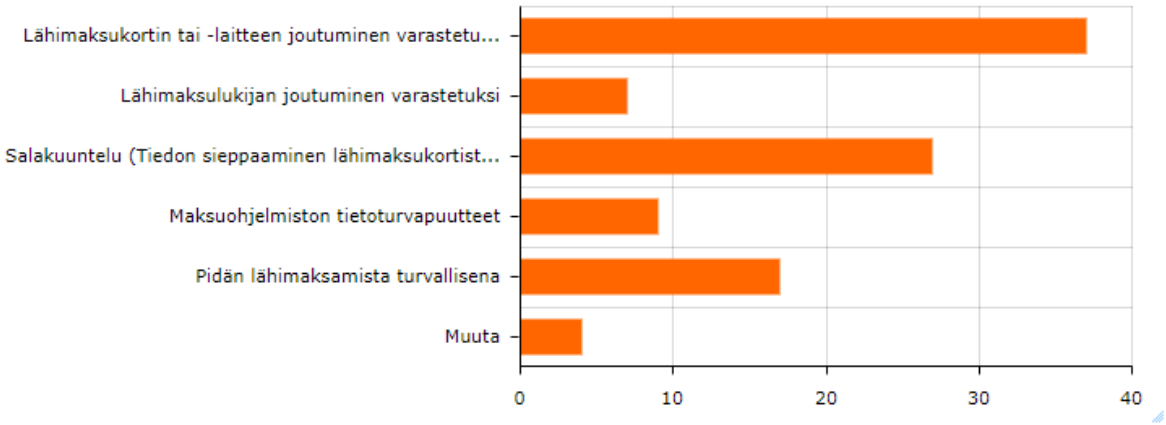
Kuvio 2. Lähimaksamisen turvallisuus

8.2 Syyt lähimaksun vaarallisuudelle

Toisella kysymyksellä pyrittiin selvittämään minkä takia vastaajat pitävät lähimaksamista vaarallisena. Kysymyksellä haluttiin selvittää mikä on vastaajien mielestä suurin tietoturvauhka lähimaksuominaisuutta käytettäessä. Tämä oli monivalintakysymys. Vastausvaihtoehdoiksi annettiin lähimaksukortin tai -laitteen joutuminen varastetuksi, lähimaksulukijan joutuminen varastetuksi, salakuuntelu (tiedon sieppaaminen lähimaksukortista tai -laitteesta), maksuohjelmiston tietoturvapuutteet, pidän lähimaksamista turvallisena, en osaa sanoa ja muu. Muu-vaihtoehto sisälsi vapaakirjoituskentän, johon vastaaja sai kirjoittaa oman vastauksensa. Kysymykseen saatiin yhteensä 67 vastausta.

Kuvion 3 mukaan 55,2 % vastaajista piti lähimaksukortin tai -laitteen joutumista varastetuksi suurimpana uhkana, joka on mielestäni myös todennäköisin tietoturvauhka. 40,3 % vastaajista piti salakuuntelua (tiedon sieppaaminen lähimaksukortista tai -laitteesta) suurimpana uhkana. Tämä oli mielestäni hieman yllättävä tulos, koska en usko että kovin moni vastaajista on tätä kokenut. Tulos perustuu luultavasti enemmänkin olettamuksiin ja uutisten luomaan väärään mielikuvaan. Lähimaksamista piti turvallisena

25,4 % vastaajista. Vastaajista 13,4 % piti maksuohjelmiston tietoturvapuutteita suurimpana uhkana. Seitsemän vastaajaa (10,4 %) piti lähimaksulukijan joutumista varastetuksi suurimpana uhkana. On hieman yllättävää että vain seitsemän vastaajan mielestä lähimaksulukijan varastaminen on suurin uhka. Uskoisin tämän olevan realistinen uhka. Vastaajat eivät välttämättä ole tietoisia siitä että varastamalla lähimaksulukija voidaan saada pääsy suuriin määriin arkaluonteista tietoa. Vastaajat eivät luultavasti pidä sitä suurena uhkana, koska se ei suoraan viittaa heidän omiin laitteisiin tai maksukortteihin. Todellisuudessa tämä varastettu lukija saattaa sisältää tiedot useista eri laitteista tai maksukorteista. 4 vastaajaa (6 %) vastasi jonkin muun syyksi. Vapaakirjoituskentän vastauksia olivat kortin lukeminen on yllättävän helppoa pidemmänkin etäisyyden päästä, MobilePay:llä rahan lähettäminen vahingossa väärään numeroon, kysymyksen vaihtoehdot epätodennäköisiä mutta mahdollisia ja yksi vastaus oli asiaton. Kukaan ei vastannut en osaa sanoa.



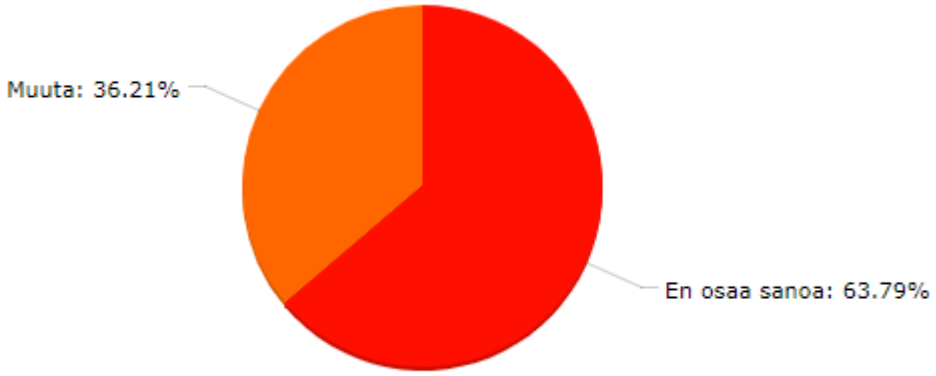
Kuvio 3. Syyt lähimaksun vaarallisuudelle

8.3 Syyt lähimaksun turvallisuudelle

Vastaajilta kysyttiin minkä takia he pitävät lähimaksamista turvallisena. Kysymyksen tuloksilla haluttiin saada selville mikä seikka vastaajien mielestä tekee lähimaksamisesta turvallista. Haluttiin myös selvittää kuinka paljon epätietoisuutta vastaajien joukossa on eli kuinka suuri osa ei osaisi nimetä yhtäkään syytä miksi lähimaksaminen on turvallista. Vaihtoehdoiksi annettiin en osaa sanoa ja pidän lähimaksamista turvallisena. Pidän lähimaksamista turvallisena-vaihtoehdossa oli vapaakirjoituskenttä, johon vastaajat saivat kertoa oman perustelunsa. 58 vastaajaa vastasi tähän kysymykseen.

Kuviosta 4 ilmenee että 2/3 (63,8 %) vastaajista ei osannut sanoa miksi pitää lähimaksamista turvallisena. Yllätyin siitä kuinka suuri osa vastaajista ei osannut perustella miksi pitää lähimaksamista turvallisena. Kysyessäni ensimmäisessä

kysymyksessä kuinka turvallista lähimaksaminen vastaajien mielestä on peräti 73,9 % vastasi joko melko turvallista tai erittäin turvallista. Mielestäni tämä kertoo ihmisten tietämättömyydestä aiheeseen ja ehkä siitä että luotetaan vain ”sokeasti” palveluntarjoajien tarjoamiin ratkaisuihin eivätkä ihmiset halua itse sen enempää miettiä turvallisuutta. 1/3 (36,2 %) vastaajista vastasi pidän lähimaksamista turvallisena. Perusteluita lähimaksamisen turvallisuudelle tuli 21 kappaletta. Suosituimpana näistä perusteluista nousi esiin maksuraja. 21 vastauksesta maksurajan tai siihen rinnastettavan vastauksen antoi 11 vastaajaa. Maksuraja on minunkin mielestäni erittäin hyvä suojauskeino väärinkäytöiltä, koska se pienentää mahdollisten taloudellisten tappioiden määrää merkittävästi. Muita yksittäisiä vastauksia olivat melko kova luotto Finteciin, luotan pankkien suunnitteluun, Suomi on yleisesti ottaen turvallinen maa, pidän huolen omista tavaroistani, ei tarvitse pin-koodia ja luotan systeemiin. Mielestäni tämäkin kertoo siitä, että ihmiset luottavat vahvasti palveluntarjoajien ratkaisuihin miettimättä itse asiaa.



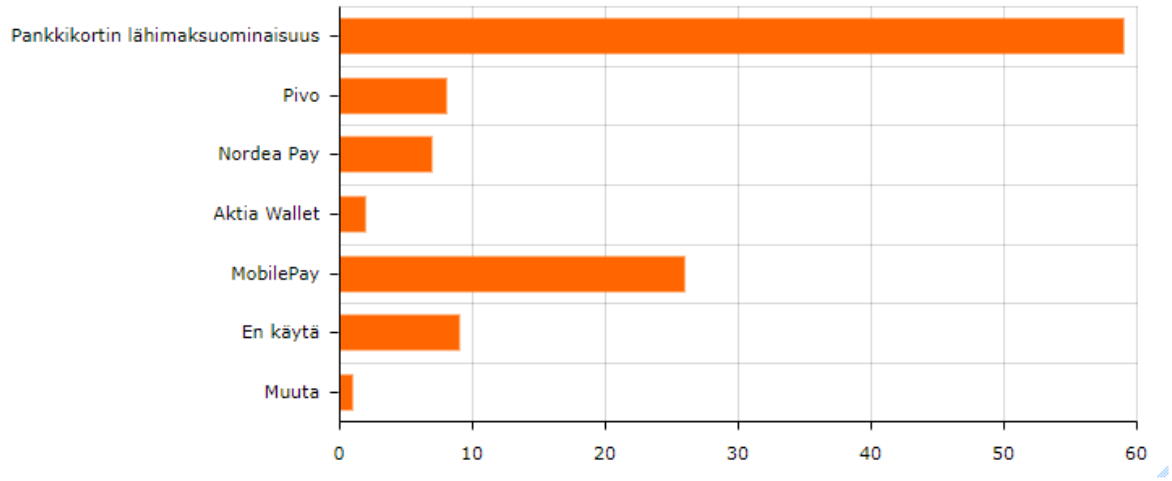
Kuvio 4. Syyt lähimaksun turvallisuudelle

8.4 Lähimaksujen eri muodot

Vastaajilta pyrittiin selvittämään mikä lähimaksumuoto on suosituin ja mikä vähiten suosittu. Lisäksi tuloksista olisi mielenkiintoista selvittää minkä pankin oma sovellus on suosituin ja onko niiden käyttömäärissä suuria eroja. Haluttiin selvittää pystyykö esimerkiksi pieni pankki kuten Aktia kilpailemaan sovelluksellaan suurien pankkien kuten Danske Bankin tai Nordean sovellusten kanssa. Lisäksi haluttiin selvittää kuinka suuri käyttäjämäärien ero on lähimaksusovelluksilla ja pankkikortin lähimaksuominaisuudella, joka on ollut paljon kauemmin jo markkinoilla. Vastausvaihtoehdoiksi annettiin pankkikortin lähimaksuominaisuus, Pivo, Nordea Pay, Aktia Wallet, MobilePay, en käytä ja muu. Muu-vastausvaihtoehdossa oli vapaakirjoituskenttä, johon vastaajat saivat kertoa

muun käytetyn lähimaksumuodon. 75 vastaajaa vastasi tähän kysymykseen. Tähän kysymykseen vastaaminen oli asetettu pakolliseksi. Kysymys oli monivalintakysymys.

Kuvion 5 mukaan vastaajista 78,7 % vastasi pankkikortin lähimaksuominaisuus. Mielestäni tämä oli odotettu tulos, koska pankkikorttien lähimaksuominaisuus on ollut useita vuosia pidempään markkinoilla kuin yksikään lähimaksusovellus. Lisäksi pankit ovat jo pidemmän aikaa myöntäneet asiakkaille oletuksena lähimaksuominaisuudella varustettuja kortteja eikä ilman kyseessä olevaa ominaisuutta varustettuja kortteja enää myönnetä. Vastaajista 34,7 % vastasi MobilePay. Mielestäni tämäkin oli odotettu tulos johtuen siitä että Danske Bank on suuri monikansallinen pankki ja heillä on suuret resurssit markkinoida omaa sovellustaan. Heillä on jo valmiina suuri asiakaskunta ja heidän on helpompi saada lisää uusia käyttäjiä MobilePay-sovellukseensa. Vain 12 % vastaajista vastasi en käytä ja tämä kertoo mielestäni lähimaksuominaisuuden kasvaneesta suosiosta. Pivo-vastauksen antoi 10,7 % vastaajista. Seitsemän vastaajaa (9,3 %) vastasi Nordea Pay. Olen hieman yllättynyt siitä että Osuuspankin Pivo on suositumpi kuin Nordean Nordea Pay. Kaksi vastaajaa (2,7 %) vastasi Aktia Wallet, joka oli odotettua koska Aktia on pienempi pankki kuin kilpailijansa. Yksi vastaaja (1,3 %) vastasi muu-vapaakirjoituskenttään Apple Pay. Tämä oli odotettua, koska Apple ei ole saanut vielä tuotua sovellustaan Apple Pay Suomen markkinoille vaikka se on jo monessa muussa maassa jo käytössä. Kun Apple Pay saa aloitettua toimintansa Suomessa uskon sen nousevan erittäin suosituksi vaihtoehdoksi johtuen Applen tuotteiden suosioista. Jos samankaltainen kysely toteutettaisiin esimerkiksi kolmen vuoden päästä nämä tulokset luultavasti eroaisivat nykyisestä.

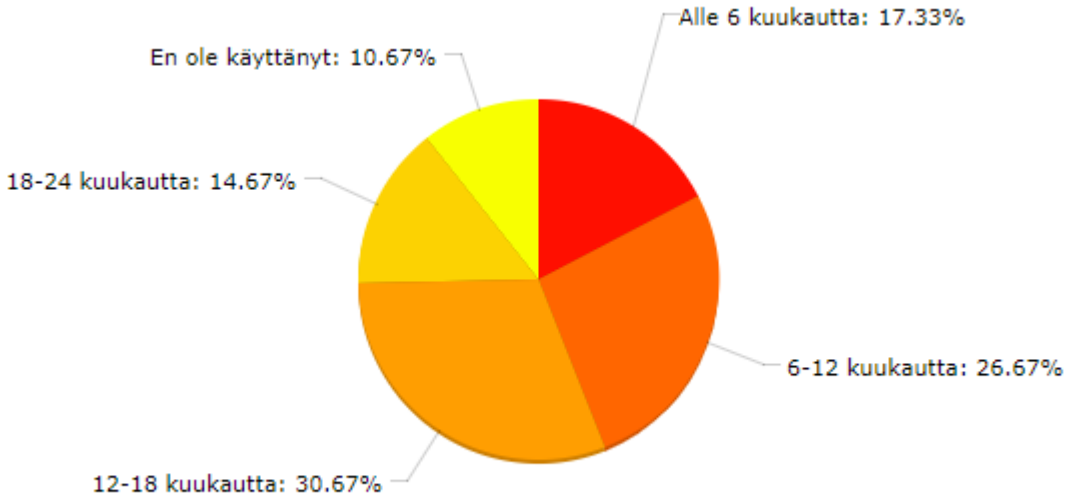


Kuvio 5. Lähimaksujen eri muodot

8.5 Lähimaksumuotojen käyttöaika

Viidennessä kysymyksessä pyrittiin selvittämään vastaajilta kuinka kauan he ovat käyttäneet lähimaksuominaisuutta. Kysymyksellä pyrittiin selvittämään myös lähimaksumuotojen suosion kehitystä. Vastausvaihtoehdoiksi annettiin alle kuusi kuukautta, 6-12 kuukautta, 12-18 kuukautta, 18-24 kuukautta, en ole käyttänyt ja muu-kuukausimäärä. Muu-vastausvaihtoehdossa oli vapaakirjoituskenttä, johon vastaaja sai kirjoittaa oman kuukausimäärän. Kysymykseen saatiin yhteensä 75 vastausta. Tähän kysymykseen vastaaminen oli asetettu pakolliseksi.

Kuviosta 6 ilmenee että 30,7 % vastaajista vastasi 12-18 kuukautta. Vastaajista 26,7 % vastasi 6-12 kuukautta. Uskon että edellä oleviin tuloksiin on vaikuttanut lähimaksusovellusten tuleminen markkinoille tuohon aikaan ja kertoo niiden suosion kasvamisesta. Alle kuusi kuukautta-vastausvaihtoehdon vastasi 17,3 % vastaajista. Tämä kertoo siitä että lähimaksusovellusten suosio kasvaa koko ajan, koska uusia käyttäjiä on tullut lisää alle kuuden kuukauden aikana. 14,7 % vastaajista vastasi kysymykseen 18-24 kuukautta. Vain kahdeksan vastaajaa (10,7 %) vastasi kysymykseen en ole käyttänyt ja mielestäni tämäkin kertoo siitä että lähimaksuominaisuus on erittäin suosittua ja lähes kaikki käyttävät sitä. Yksi tutkimuksen hypoteeseista oli lähimaksupalveluiden käyttö lisääntyy koko ajan ja tutkimuksen tulokset tukevat hypoteesia vahvasti. Kukaan ei vastannut muu-kuukausimäärää.

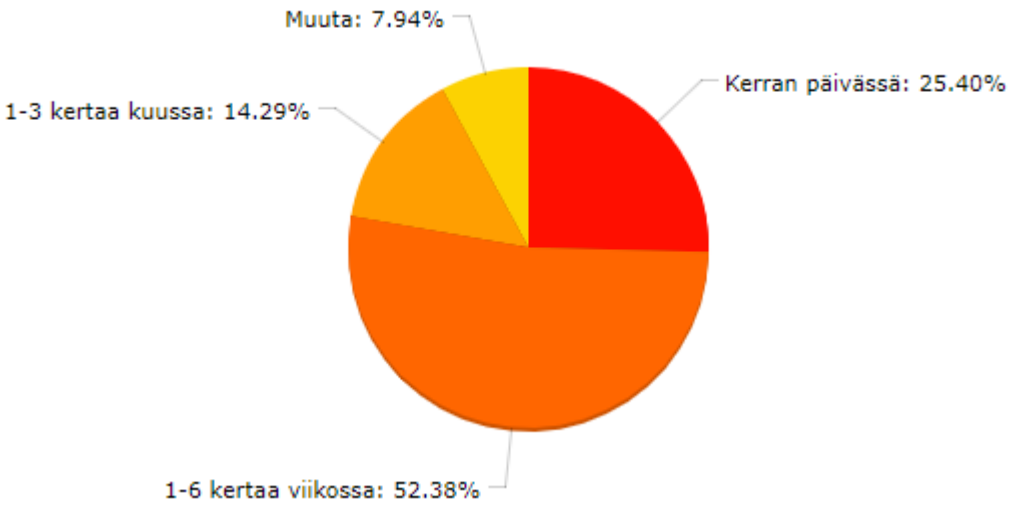


Kuvio 6. Lähimaksumuotojen käyttöaika

8.6 Lähimaksumuotojen käyttötiheys

Kuudennessa kysymyksessä pyrittiin selvittämään kuinka usein vastaajat käyttävät lähimaksuominaisuutta. Kysymyksellä pyrittiin selvittämään lähimaksumuotojen käyttötiheyttä ja suosiota. Vastausvaihtoehdoiksi annettiin kerran päivässä, 1-6 kertaa viikossa ja 1-3 kertaa kuussa. Vaihtoehtona oli lisäksi useita kertoja päivässä, johon vastaaja sai kirjoittaa vapaakirjoituskenttään oman määränsä. Kysymyksessä kehotettiin vastaajia jättämään vastaamatta, jos he eivät olleet käyttäneet lähimaksuominaisuutta. Vastauksia kysymykseen tuli yhteensä 63 kappaletta.

Kuvion 7 mukaan vastaajista selkeä enemmistö 52,4 % vastasi kysymykseen 1-6 kertaa viikossa. 25,4 % vastaajista vastasi kerran päivässä. Eli vastaajista peräti 77,8 % käyttää lähimaksuominaisuutta 1-6 kertaa viikossa tai kerran päivässä. Tuloksista voidaan päätellä että lähimaksuominaisuus on lähes kaikkien vastaajien ensisijainen maksuväline. 1-3 kertaa kuussa-vastausvaihtoehdon valitsi 9 vastaajaa (14,3 %). Muu-vapaakirjoituskenttään kirjoitti 5 vastaajaa (7,9 %). Vapaakirjoituskentän vastauksia olivat aina alle 25e ostoksissa, 1-4 kertaa päivässä, 2-5 kertaa päivässä, 1-5 kertaa päivässä ja 2-3 kertaa päivässä.



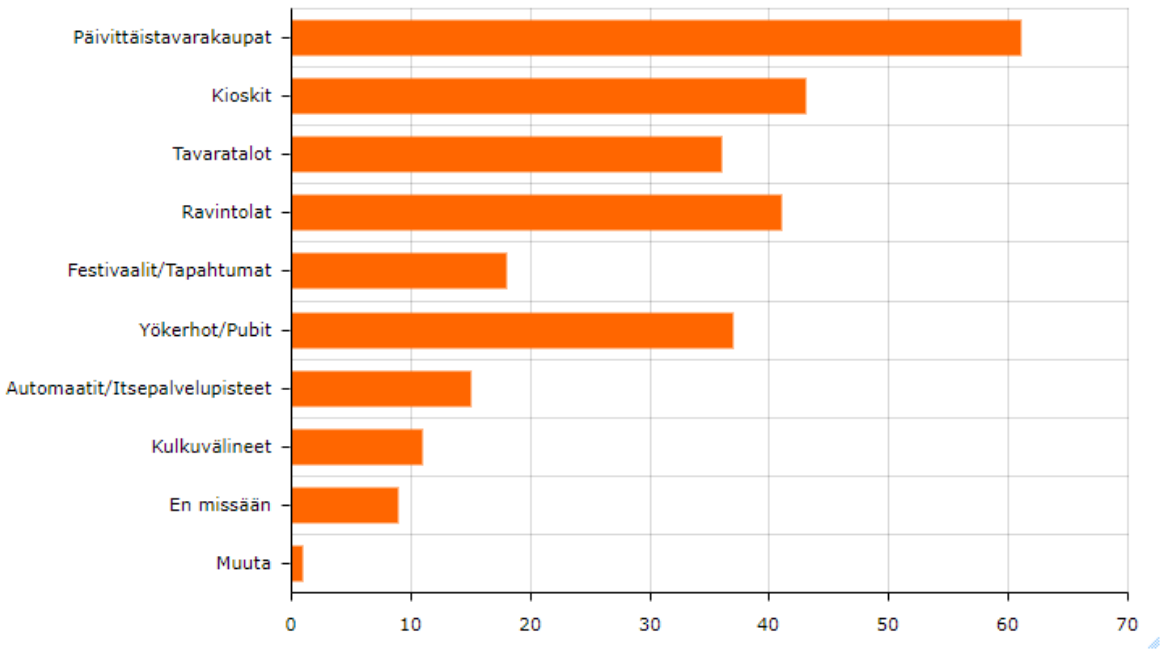
Kuvio 7. Lähimaksumuotojen käyttötiheys

8.7 Lähimaksuominaisuuden käyttöpaikat

Vastaajilta kysyttiin missä he käyttävät lähimaksuominaisuutta. Kysymyksellä pyrittiin selvittämään mikä on suosituin lähimaksuominaisuuden käyttöpaikka ja minkälaisia eroja eri käyttöpaikkojen välille syntyy. Haluttiin myös selvittää tuleeko kenties jotain yllättäviä vaihtoehtoja esiin. Vastausvaihtoehdoiksi annettiin päivittäistavarakaupat, kioskit, tavaratalot, ravintolat, festivaalit/tapahtumat, yökerhot/pubit, automaatit/itsepalvelupisteet,

kulkuvälineet, en missään ja muu-vapaakirjoituskenttä, johon vastaaja sai kirjoittaa itse paikan jossa lähimaksuominaisuutta käyttää. Kysymykseen vastaaminen oli asetettu pakolliseksi. Vastauksia saimme kysymykseen yhteensä 74 kappaletta. Kysymys oli monivalintakysymys.

Kuviosta 8 ilmenee että suosituin vastaus oli päivittäistavarakaupat, jonka vastasi 61 vastaajaa. Mielestäni tämä oli odotettu tulos, koska päivittäistavarakaupoissa asioidaan eniten. Toiseksi suosituin käyttöpaikka oli kioskit, jonka vastasi 43 vastaajaa. Tämäkin oli mielestäni odotettua, koska kioskeilla asioidaa usein ja etenkin pienet maksut on kätevä hoitaa lähimaksuominaisuudella nopeasti ilman tunnusluvun näppäilyä. Heti kioskien perässä tuli ravintolat 41 vastauksella. 37 vastaajaa vastasi kysymykseen yökerhot/pubit. Tavaratalot saivat 36 vastausta. Festivaalit/tapahtumat saivat vastaajilta 18 vastausta. Ihmiset käyvät luultavasti suhteellisen harvoin festivaaleilla ja tapahtumissa ja siksi tämäkin tulos oli odotettu. 15 vastaajaa vastasi automaatit/itsepalvelupisteet. 11 vastaajaa vastasi kulkuvälineet. Uskon että tulevaisuudessa lähimaksuominaisuuden käyttö tulee kasvamaan selkeästi kulkuvälineissä. Vain yhdeksän vastaajaa vastasi etteivät käytä lähimaksuominaisuutta missään. Tämäkin tukee jo aiemmissa tuloksissa esiintynyttä ilmiötä siitä että lähimaksuominaisuuden suosio on tällä hetkellä korkea. Yksi vastaaja vastasi vapaakirjoituskenttään ystävien kesken, kirpputoreilla ja rahansiirtoihin yksityishenkilöille.



Kuvio 8. Lähimaksuominaisuuden käyttöpaikat

9 Pohdinta

Tutkimukseni mukaan suurin osa ihmisistä pitää lähimaksamista melko turvallisena ja tämä tukee myös tutkimuksen hypoteesia ihmiset suhtautuvat lähimaksupalveluihin pääosin positiivisesti mutta ne herättävät ihmisissä myös huolta ja negatiivisia tunteita. Ihmiset pitävät maksurajaa tärkeimpänä turvallisuustekijänä. Tämä on minunkin mielestä erittäin hyvä keino ehkäistä väärinkäytöksiä, koska taloudelliset menetykset pysyvät hyvin pieninä maksurajan takia. Suurimpana turvallisuusuhkana lähimaksupalveluissa ihmiset pitävät lähimaksukortin tai -laitteen joutumista varastetuksi. Mielestäni tulos on odotettu ja se on kaikista todennäköisin turvallisuusuhka. Tutkimukseni mukaan pankkikortin lähimaksuominaisuus on ylivoimaisesti käytetyin lähimaksumuoto sillä vastaajista 78,7 % vastasi käyttävänsä sitä. Tutkiessani kuinka kauan ihmiset ovat lähimaksuominaisuutta käyttäneet selvisi, että eniten sitä on käytetty 12-18 kuukautta. Uskon sen johtuvan lähimaksusovellusten tulemisesta markkinoille tuohon aikaan. Tulos tukee myös tutkimuksen hypoteesia lähimaksupalveluiden käyttö lisääntyy koko ajan. Lähimaksupalveluiden suosiosta kertoo se, että suurin osa ihmisistä käyttää lähimaksuominaisuutta 1-6 kertaa viikossa. Mielestäni tuloksista ilmenee se että suurin osa vastaajista käyttää lähimaksuominaisuutta ensisijaisena maksuvälineenä. Lähimaksuominaisuutta käytetään selkeästi eniten päivittäistavarakaupoissa. Tämä johtunee siitä että päivittäistavarakaupoissa asioidaan yleensä eniten.

9.1 Tulosten luotettavuus

Tähän kyselytutkimukseen vastasi 75 vastaajaa. Se on hyvin pieni määrä verrattuna siihen että Suomessa NFC-ominaisuudella varustettuja lähimaksukortteja on jo noin 3 miljoonaa kappaletta ja kymmeniä tuhansia niiden vastaanottamiseen aktivoituja maksupäätteitä. On huomioitava että jokaiseen kysymykseen eivät vastanneet kaikki 75 vastaajaa. Neljässä kysymyksessä oli mahdollisuus ohittaa kysymys vastaamatta siihen. Tämä siksi että kysymyksiin haluttiin vastaus vastaajilta, jotka olivat lähimaksumuotoja käyttäneet. Muutoin kysymysten tuloksiin olisi tullut mukaan olettamuksia vastaajilta joilla ei ollut asiasta kokemusta.

Tämä tutkimus antaa merkin siitä että ihmiset pitävät pääosin lähimaksamista melko turvallisena sillä yli puolet vastaajista (57,97 %) vastasi näin. Luotettavana voidaan pitää myös tietoa siitä, että lähimaksukortin tai -laitteen joutuminen varastetuksi on suurin turvallisuusuhka lähimaksuominaisuutta käytettäessä. Yli puolet vastaajista (55,2 %) oli tätä mieltä. Tämä tutkimus antaa merkin siitä, että pankkikortin lähimaksuominaisuus on käytetyin lähimaksumuoto sillä peräti 78,7 % vastaajista vastasi näin. On huomioitava

kuitenkin että otos on pieni. Tämän tutkimuksen tulokset viittaavat siihen, että suurin osa ihmisistä käyttää lähimaksumuotoja 1-6 kertaa viikossa. Näin vastasi 52,38 % vastaajista. Mutta on huomioitava otoksen pieni koko. Lähimaksuominaisuuden suosituimmaksi käyttöpaikaksi voidaan luotettavasti sanoa päivittäistavarakaupat, johtuen 61:n vastaajan kertomasta täydestä 74 vastauksen määrästä.

Kyselyssä ei selvitetty vastaajien ikää eikä sukupuolta. Tämä olisi voinut tuoda lisäarvoa tuloksiin, koska nuorten ja vanhempien ihmisten mielipiteet ja kokemukset luultavasti eroaisivat toisistaan jonkin verran. Nuoret, jotka ovat eläneet suurimman osan elämästään digitalisaation aikana omaavat luultavasti erilaisen mielipiteen kuin vanhemmat ihmiset. Vanhemmilla ihmisillä, jotka eivät ole teknisesti kovin orientoituneita mielipiteisiin voi vaikuttaa tietämättömyys ja usein tuntematon ja uusi voi tuntua epämiellyttävältä sekä vaaralliselta. Etenkin kun tutkimme niinkin tärkeää asiaa kuin rahamaksujen turvallisuus. Kyselyyni vastanneet olivat pääosin Facebook-kavereitani ja iältään noin 20-30 vuotiaita. Kysely levisi vanhempieni toimesta heidän kollegoilleen, jotka ovat iältään noin 50-vuotiaita. Tuloksista ei voida sanoa eroavatko noin 20-30 vuotiaiden mielipiteet noin 50-vuotiaiden mielipiteistä. En pysty arvioimaan, kuinka moni noin 50-vuotias on kyselyyni vastannut.

9.2 Tulosten analysointi ja hypoteesien tukeminen

Tutkimukseni mukaan ihmisten mielestä lähimaksaminen on melko turvallista. Vain yhden vastaajan mielestä 69:n joukosta lähimaksaminen on erittäin vaarallista. Kolme vastaajaa 69:n joukosta ei osannut sanoa kuinka turvallista lähimaksaminen heidän mielestään on. Tämä kertoo mielestäni siitä, että suurin osa vastaajista on perehtynyt lähimaksamiseen ja he pystyvät muodostamaan itsenäisen mielipiteen aiheesta.

Suurimpana turvallisuusuhkana lähimaksamisessa vastaajat pitävät lähimaksukortin tai -laitteen joutumista varastetuksi. Tämä voi seurata omasta huolimattomasta käytöksestä tai esimerkiksi taitavasta taskuvarkaasta. Käyttäjä altistuu tälle vaaralle periaatteessa aina kun poistuu kodistaan. Pankkien asettama 25 euron maksuraja tekee väärinkäytöistä vaikeampaa väärinkäyttäjille. Jos mobiililaite varastetaan lähimaksusovellus ei ole välttämättä edes suurin huolenaihe. Älypuhelimet voivat sisältää paljon yksilöllistä tietoa käyttäjästään ja näin ollen sieltä voi löytyä arvokkaampaakin varastettavaa kuin esimerkiksi pieni summa rahaa. Älypuhelimissa on syytä pitää päällä vähintään yhtä lukitusmekanismia, kuten numerokoodia, pääsykuviota tai sormenjälkitunnistusta. Tämä vaikeuttaa väärinkäyttöä. Lisäksi älypuhelin on mahdollista paikantaa

kirjautumistunnuksilla sen kadotessa. Tai sen voi lukita etänä. Nämä seikat parantavat myös turvallisuutta.

Toiseksi suurimpana turvallisuusuhkana lähimaksamisessa ihmiset pitävät salakuuntelua eli tiedon sieppaamista lähimaksukortista tai -laitteesta. Puhuttaessa mobiililaitteesta, jolla tehdään lähimaksuja on syytä pitää NFC-ominaisuus pois päältä aina kun sitä ei tarvita. Tämä ehkäisee väärinkäyttöjä. Lähimaksukortin suojaamiseen monet palveluntarjoajat myyvät RFID-suojauksella varustettuja kopioinnilta suojaavia korttikoteloita. Näin pystytään myös ehkäisemään salakuuntelua. Kysyttäessä miksi vastaajat pitävät lähimaksamista vaarallisena kukaan ei vastannut en osaa sanoa. Tämä voi kertoa siitä että ihmiset ovat perehtyneet lähimaksamisen mahdollisiin tietoturvauhkiin ja tiedostavat mikä oikeasti uhkaa turvallisuutta. Kolmanneksi suosituin vastaus oli pidän lähimaksamista turvallisena.

Kysyttäessä minkä takia ihmiset pitävät lähimaksamista turvallisena peräti 63,8 % vastaajista vastasi en osaa sanoa. Aiemmat tulokset ovat viitanneet siihen, että ihmiset ovat hyvin perillä lähimaksamisesta. Tämä tulos sen sijaan viittaa vahvasti epätietoisuuteen, koska suurin osa ihmisistä ei osannut perustella miksi pitää lähimaksamista turvallisena. Mielestäni tämä viittaa siihen että suurin osa ihmisistä ymmärtää lähimaksupalvelut kokonaisuutena ja pitävät niitä pääosin turvallisina mutta he eivät osaa tarkemmin perustella valintaansa. Vastaajien mielestä maksuraja oli tärkein turvallisuutta nostava tekijä.

Selkeästi suosituin käytetty lähimaksumuoto on pankkikortin lähimaksuominaisuus. Tämä johtuu siitä, että se on ollut pisimpään asiakkaiden saatavilla ja pankit oletuksena antavat asiakkaille lähimaksuominaisuudella varustettuja pankkikortteja. Toiseksi suosituin lähimaksumuoto oli tutkimukseni mukaan MobilePay, koska 34,7 % vastaajista vastasi näin. Vaikuttaisi siltä, että MobilePay on saanut vakiinnutettua parhaimman markkina-aseman kilpailijoihinsa nähden. MobilePay on Danske Bankin sovellus. Yksi tavoite oli selvittää minkä pankin sovellus on suosituin. Ero esimerkiksi toisen suuren pankin Nordean sovellukseen Nordea Pay on suuri. Nordea Pay:n vastasi vain 7 vastaajaa, kun MobilePay:n vastasi 26 vastaajaa.

Kysyttäessä vastaajilta kuinka kauan he ovat lähimaksuominaisuutta käyttäneet 30,7 % vastaajista vastasi käyttäneensä lähimaksuominaisuutta 12-18 kuukautta. Toiseksi suosituin vastaus oli 6-12 kuukautta, jonka vastasi 26,67 % vastaajista. Tämä johtuu lähimaksusovellusten tulemisesta markkinoille vuonna 2016. Tutkimukseni perusteella lähimaksuominaisuuden käyttö on suosittua, koska vain 10,7 % vastaajista vastasi etteivät

ole lähimaksuominaisuutta käyttäneet. Kysymykseen vastasi 75 vastaajaa, joka on pieni määrä verrattuna siihen että lähimaksuominaisuudella varustettuja maksukortteja on Suomessa käytössä noin 3 miljoonaa kappaletta.

Lähimaksupalveluiden suosiosta kertoo myös se, että vastaajista hieman yli puolet (52,4 %) kertoo käyttävänsä lähimaksuominaisuutta 1-6 kertaa viikossa. Vastaajista 25,4 % kertoo käyttävänsä lähimaksuominaisuutta kerran päivässä. Tämän lisäksi vajaa kymmenosa (7,6 %) vastaajista kertoo käyttävänsä lähimaksuominaisuutta useita kertoja päivässä. Nämä tutkimustulokset viittaavat siihen, että lähimaksuominaisuuden käyttäminen on erittäin suosittua.

Lähimaksuominaisuutta käytetään selkeästi eniten päivittäistavarakaupoissa. Tämä oletettavasti johtuu siitä, että päivittäistavarakaupoissa asioidaan muutenkin usein. Muita suosittuja käyttöpaikkoja lähimaksuominaisuudelle ovat kioskit, ravintolat ja yökerhot/pubit. Vain yhdeksän vastaajaa ilmoitti ettei käytä lähimaksuominaisuutta missään. Mielestäni tämäkin seikka kertoo siitä, että lähimaksupalvelut ovat hyvin käytettyjä nykyään.

Yksi tutkimukseni hypoteeseista oli, että lähimaksupalveluiden käyttö lisääntyy koko ajan. Tutkimukseni tulokset viittaavat tähän hyvin vahvasti. Tekemästäni kyselystä on selvinnyt, että lähimaksupalveluita käytetään hyvin paljon. Vain 12 % vastaajista ilmoitti, ettei käytä lähimaksupalveluita. Kun otamme huomioon sen, että lähimaksaminen lähimaksusovelluksilla tuli mahdolliseksi vasta vuonna 2016 näyttää siltä, että hyvin lyhyessä ajassa käyttö on kasvanut suureksi. Vastaajista 58,7 % kertoi käyttävänsä jotakin lähimaksusovellusta.

Toinen tutkimukseni hypoteeseista oli, että lähimaksupalveluiden käytön lisääntyessä tietoturvamurrot ja väärinkäytöt lisääntyvät. Tämän kyselyn mukaan näin ei ole. Vastaajista 58 % oli sitä mieltä, että lähimaksaminen on melko turvallista. Vain yhden vastaajan (1,4 %) mukaan lähimaksaminen on erittäin vaarallista. Jos lähimaksupalveluiden käytön lisääntyessä tietoturvamurrot ja väärinkäytöt lisääntyisivät tämä todennäköisesti kävisi ilmi kyselystäni siten, että vastaajien mielestä lähimaksaminen olisi vaarallisempaa. Tutkimuksestani ei käy ilmi tämän suuntaisia tietoturvamurtoja tai väärinkäyttöjä. Ihmisten mielipiteet olisivat enemmän vaarallisen puolella, koska useampi olisi kokenut tietoturvamurtoja tai väärinkäyttöjä.

Kolmannen hypoteesin mukaan ihmiset suhtautuvat lähimaksupalveluihin pääosin positiivisesti, mutta ne herättävät ihmisissä myös huolta ja negatiivisia tunteita. Kyselyni

tulokset tukevat tätä hypoteesia. Vastaajista 58 % kertoi lähimaksamisen olevan melko turvallista heidän mielestään. Tämä tukee hypoteesin väitettä, että ihmiset suhtautuvat lähimaksupalveluihin pääosin myönteisesti. Lähimaksaminen herättää myös hieman huolta ja negatiivisia tunteita. Vastaajista 20,3 % ilmoitti, että heidän mielestään lähimaksaminen on hieman vaarallista. Suurimmat huolen aiheet olivat lähimaksukortin tai -laitteen joutuminen varastetuksi ja salakuuntelu eli tiedon sieppaaminen lähimaksukortista tai -laitteesta.

9.3 Johtopäätökset

Tutkimustulosten pohjalta voidaan tehdä johtopäätös, että lähimaksupalvelut ovat nousseet lyhyessä ajassa erittäin käytetyiksi. Vastaajista 74,67 % on aloittanut lähimaksuominaisuuden käytön 18 kuukauden sisällä. Tähän on varmasti monia syitä, jotka voivat olla ainakin älypuhelinten käytön lisääntyminen ja pankkien oletuksena myöntämät lähimaksuominaisuuden omaavat pankkikortit. On mielenkiintoista nähdä jatkuuko lähimaksupalveluiden käytön lisääntyminen samaa vauhtia tulevaisuudessa vai onko tämä vain uutuuden viehätystä ja kokeilua.

Kyselyyn vastanneista selkeä enemmistö (73,9 %) pitää lähimaksamista erittäin turvallisena tai melko turvallisena. Tämä viittaa siihen, että ihmiset eivät ole pääosin ainakaan kokeneet tietoturvamurtoja tai väärinkäytöksiä. Lähimaksaminen herättää myös huolta.Tästä kertoo kyselyn tulos, jossa 20,3 % vastaajista kertoo lähimaksamisen olevan hieman vaarallista heidän mielestään. On vaikea sanoa johtuvatko nämä negatiiviset tunteet tietämättömyydestä vai oikeista kokemuksista.

Tämän kyselyn tulosten pohjalta voidaan tehdä johtopäätös, että suurimmat turvallisuusuhat lähimaksamisessa kyselyn perusteella ovat lähimaksukortin tai -laitteen joutuminen varastetuksi ja salakuuntelu eli tiedon sieppaaminen lähimaksukortista tai -laitteesta. Tekemäni kyselytutkimuksen pohjalta on mahdotonta sanoa perustuvatko nämä mielipiteet oikeasti koettuun uhkaan vai ovatko ne vain ihmisten olettamuksia, koska se ei tuloksista ilmene. NFC:n mahdollisia tietoturvauhkia tutkittuani pidän myös lähimaksukortin tai -laitteen joutumista varastetuksi ja salakuuntelua todennäköisimpinä uhkina. Ne on huomattavasti helpompi toteuttaa kuin esimerkiksi suuren budjetin, kalliin laitteiston ja asiantuntevan tekijän vaativa invasiivinen hyökkäys. Puhuttaessa eniten tuhoa aikaansaavista hyökkäyksistä on mainittava NFC-lukijan varastaminen. NFC-lukijan varastamalla hyökkääjä voi päästä käsiksi useiden eri laitteiden arkaluontoisiin tietoihin. NFC-lukijan varastamista pidetään vaarallisempana uhkana kuin lähimaksukortin tai -laitteen joutumista varastetuksi, siitä saatavan suuremman tietomäärän vuoksi.

Lähimaksukortin tai -laitteen joutuminen varastetuksi on todennäköisempää kuin NFC-lukijan varastaminen, koska NFC-lukija on sijoitettu fyysisesti vartioidulle alueelle. Lähimaksukortit ja -laitteet voivat joutua helpommin varastetuksi ihmisten huolimattomuudesta johtuen. Ihmisen liikkuessa esimerkiksi kaupungilla älypuhelimen kanssa sen todennäköisyys joutua varastetuksi on suurempi kuin ihmisen ollessa kotona.

Tutkiessani kyselyssä ilmenneitä perusteluita lähimaksamisen turvallisuudelle esiin nousivat maksuraja sekä seikka, että pin-koodia ei tarvitse antaa lähimaksua suoritettaessa. Alhainen 25 euron maksuraja estää ainakin suuria kertaväärinkäytöksiä. Se, että pin-koodia ei tarvitse näppäillä lähimaksuissa, vähentää todennäköisyyttä sen joutumisesta vääriin käsiin. Toisaalta, jos pin-koodia ei tarvitse näppäillä varastetulla kortilla väärinkäyttäjän on helppo ostaa pieniä alle 25 euron ostoksia. Pankit ovat tosin tähänkin varautuneet. Lähimaksukorttia käytettäessä maksupääte pyytää satunnaisesti ostajaa laittamaan kortin sirun lukijaan ja näppäilemään pin-koodin. Tällä tavalla pyritään vähentämään väärinkäytöksiä. Useat palveluntarjoajat myös markkinoivat asiakkailleen suojakoteloa maksukorteille, joita radioaallot eivät läpäise. Käytettäessä lähimaksuominaisuudella varustettua pankkikorttia on turvallisempaa käyttää edellä mainittua suojakoteloa mieluummin kuin perinteistä lompakkoa. Perinteistä lompakkoa käytettäessä esimerkiksi salakuuntelun uhriksi joutuminen on todennäköisempää kuin radioaalloilta suojattua suojakoteloa käytettäessä, koska perinteinen lompakko ei suojaa salakuuntelulta millään tavoin. Älypuhelimiin asetettavat suojamekanismit kuten suojakoodi ja sormenjälkitunnistus tekevät väärinkäytöksien suorittamisesta vaikeampaa. Väärinkäytöiltä ja tietoturvamurroilta suojaa myös kun NFC-ominaisuus pidetään suljettuna mobiililaitteessa aina kun sitä ei käytetä. NFC-ominaisuuden ollessa tarpeettomasti päällä mobiililaitteessa todennäköisyys joutua tietoturvamurron uhriksi kasvaa etenkin liikuttaessa vilkkaissa paikoissa kuten kaupungissa. Omista henkilökohtaisista tavaroista huolehtiminen on tärkein tekijä, kun pyritään lisäämään turvallisuutta. Väärinkäyttäjän on helppo varastaa esimerkiksi lähimaksuominaisuudella varustettu mobiililaite, jos käyttäjä ei pidä sitä valvonnan alla.

Pankkikortin lähimaksuominaisuus on eniten käytetty lähimaksumuoto. Näin ilmoitti 59 vastaajaa 75 vastaajasta. Tämä johtuu siitä, että pankkien lähimaksuominaisuudella varustetut pankkikortit ovat olleet markkinoilla useita vuosia pidempään kuin älypuhelinten lähimaksusovellukset. Älypuhelinten lähimaksusovellusten lähimaksuominaisuus tuli markkinoille vasta vuonna 2016. Tutkimukseni tavoitteena oli myös selvittää minkä pankin sovellus on suosituin ja minkälaisia eroja niiden välillä syntyy. Lähimaksusovelluksista käytetyin on Danske Bankin MobilePay. Kyselytutkimuksessani sitä vastasi käyttävänsä 34,7 % vastaajista. MobilePay on saanut hyvin lyhyessä ajassa paljon käyttäjiä kun

otetaan huomioon sen lähimaksuominaisuuden tuleminen mahdolliseksi vasta vuonna 2016. Muut sovellukset kuten OP:n Pivo (10,7 %), Nordean Nordea Pay (9,3 %) ja Aktian Aktia Wallet (2,7 %) ovat huomattavasti vähemmän käytettyjä. Tulevaisuudessa on mielenkiintoista nähdä tasoittuvatko käyttäjämäärien väliset erot eri sovelluksissa vai jatkaako MobilePay selkeässä johdossa. Applen Apple Pay:tä vastasi käyttävänsä vain 1,3 % vastaajista. Apple ei ole vielä saanut omaa versiotaan käyttöön Suomen markkinoille vaikka se on jo useissa muissa maissa käytössä. Applen päästessä kilpailuun mukaan sen käyttö tulee todennäköisesti kasvamaan johtuen Applen mobiililaitteiden suosiosta.

Tutkimustulosten pohjalta voidaan sanoa, että suurin osa ihmisistä (30,6 %) on aloittanut lähimaksuominaisuuden käytön 12-18 kuukautta sitten. Tämä aika sijoittuu siis vuoteen 2016, jolloin lähimaksusovellusten lähimaksuominaisuus tuli mahdolliseksi. Voidaan siis sanoa, että lähimaksusovellusten myötä lähimaksuominaisuuden käyttö on lisääntynyt.

Tämän kyselyn tulosten pohjalta voidaan tehdä johtopäätös, että vastaajat käyttävät lähimaksuominaisuutta aktiivisesti. Suurin osa ihmisistä (52,4 %) käyttää lähimaksuominaisuutta 1-6 kertaa viikossa. Suurin osa ihmisistä (61 vastaajaa 74:stä) käyttää lähimaksuominaisuutta päivittäistavarakaupoissa. Tämä johtuu siitä, että päivittäistaravakaupoissa asioidaan muutenkin usein verrattuna esimerkiksi ravintoloihin (41 vastaajaa) tai festivaaleihin/tapahtumiin (18 vastaajaa).

9.4 Kehitys- ja jatkotutkimusehdotukset

Tässä tutkimuksessa olisi voitu kysyä vastaajilta ikä. Tämä olisi voinut tuoda lisäarvoa tuloksiin, koska on mahdollista että nuorempien ja vanhempien ihmisten käyttötavat ja mielipiteet turvallisuusasioista olisivat voineet erota toisistaan.

Tämä tutkimus on tehty suomen kielellä ja siihen vastanneet asuvat Suomessa. Saman kaltainen tutkimus voitaisiin tehdä toisessa maassa ja näin verrata millä tavoin lähimaksupalveluiden käyttö ja tietoturvauhat eroavat Suomen ja toisen maan välillä vai löytyykö niistä yhteneväisyyksiä.

Suunnitellessani opinnäytetyötä ideana oli haastatella sekä palveluntarjoajia, että käyttäjiä. Tässä opinnäytetyössä päädyttiin tutkimaan vain käyttäjien mielipiteitä ja kokemuksia, koska tutkimus olisi laajentunut liikaa jos palveluntarjoajien näkymykset olisi otettu mukaan. Palveluntarjoajien haastatteluilla voitaisiin teettää kokonaan uusi tutkimus

ja esimerkiksi verrata ovatko asiakkaiden ja palveluntarjoajien näkemykset samankaltaisia.

9.5 Oman oppimisen arviointi

Tätä opinnäytetyötä tehdessäni kielitaitoni on kohentunut selkeästi, koska lähes kaikki tutkimani lähteet oli kirjoitettu englanniksi. Tutkiessani aihetta olen oppinut ymmärtämään hyvinkin teknistä sanastoa paremmin. Tätä työtä tehdessäni olen kehittänyt tieteellistä kirjoittamista, jota juurikaan en ollut aiemmin tehnyt. Tämä oli myös ensimmäinen kerta, kun olen tehnyt tutkimusta. Tämän myötä olen oppinut paljon uutta haastattelukysymyksien suunnittelusta ja haastattelututkimuksen läpiviennistä. Haastattelukysymyksien suunnittelussa on tärkeää suunnitella huolellisesti kysymysten loogisuus, jotta tulokset eivät ole ristiriidassa keskenään ja päätelmiä tuloksista voidaan tehdä. Haastattelututkimuksen läpiviennissä ymmärsin että kysymysten täytyy olla helposti ymmärrettäviä sekä nopeasti vastattavia, jotta saadaan mahdollisimman paljon analysoitavia tuloksia. Tämän työn myötä opin, kuinka haastattelututkimuksen tuloksia tulee analysoida ja mitä niistä voidaan päätellä. Kehitin tämän prosessin aikana myös lähteiden etsimistaitojani huomattavasti. Opin myös lähteiden luotettavuuden arviointia. Tällä tarkoitan sitä että lähteen täytyy perustua tutkittuun tietoon ja mitä laajemmasta tutkimuksesta on kysymys sitä luotettavampia tulokset ovat.

Minulla ei ollut syvällistä tietoa NFC-tekniikasta ja lähimaksuominaisuudesta, kun aloitin tämän työn. Itse NFC-tekniikan toimintalogiikkaa olen oppinut ymmärtämään enemmän teknisellä tasolla. Olen oppinut että NFC perustuu RFID-tekniikkaan mutta NFC on rajoitettu toimimaan lyhyemmällä etäisyydellä. NFC-teknologialla voidaan mahdollistaa kahden laitteen välinen kommunikointi langattomasti muutaman senttimetrin etäisyydellä. Kommunikointi tapahtuu 13,56 MHz:n tajuudella samoin kuin RFID:ssä. NFC-teknologian avulla voidaan mahdollistaa kahden NFC-laitteen välillä lyhyen kantaman, korkean taajuuden ja matalan tiedonsiirtonopeuden langaton tiedonsiirto. Opin uutta NFC-tekniikan haavoittuvuuksista ja erilaisista hyökkäys- ja tiedonkalastusmetodeista. Opin ymmärtämään enemmän haavoittuvuuksista, jotka liittyvät NFC-tagiin, NFC-lukijaan, älykorttiin, kommunikointiin sekä väliohjelmistoon ja backend-järjestelmiin.

Opin esimerkiksi sen että NFC-tagin hyökkäykset voidaan jaotella kolmeen eri ryhmään: tagin kloonaukseen/imitointiin, tagin sisällön muuttamiseen ja tagin vaihtamiseen/piilottamiseen. NFC-lukijan hyökkäykset voidaan jaotella kahteen eri ryhmään, jotka ovat NFC-lukijan poistaminen/tuhoaminen ja imitointi. Älykorttien hyökkäykset puolestaan voidaan jakaa kahteen eri ryhmään eli invasiivisiin hyökkäyksiin

ja sivukanavan hyökkäyksiin. Kommunikaation aikana tapahtuvia hyökkäysvaihtoehtoja on viisi kappaletta. Ne ovat salakuuntelu, tiedon korruptointi, tiedon muuttaminen, tietojen syöttö ja mies välissä-hyökkäys. Opin myös sen että käsiteltäessä NFC-teknologian haavoittuvuuksia tulee ottaa huomioon väliohjelmiston ja backend-järjestelmän turvallisuus. Kaikkien NFC-järjestelmän osien kuten pankkipalvelimien, luottokorttiväliohjelmiston ja autentikointi-osajärjestelmien täytyy olla suojattu, jotta saavutetaan mahdollisimman monipuolinen suojaus hyökkäyksiä vastaan. Erittäin tärkeänä pidän oppimiani asioita liittyen NFC-tekniikkaan, joilla voidaan ehkäistä tietomurtoja ja hyökkäyksiä. Kommunikaation tärkein suojauskeino on suojatun kanavan perustaminen. Muita suojauskeinoja ovat NFC:n kytkeminen pois päältä kun sitä ei käytetä ja lähimaksukortin säilyttäminen radioaalloilta suojatussa kotelossa. Erittäin tärkeää on myös huolehtia omista yksityisistä tavaroistaan kuten lähimaksuominaisuudella varustetusta matkapuhelimesta ja lähimaksukortista, jotta ne eivät joudu väärinkäytetyiksi. Olen oppinut myös miten erilaiset Suomessa tarjolla olevat lähimaksupalvelut eroavat toisistaan.

Itse opinnäytetyöprosessi on ollut pitkä mutta opettavainen. Olen oppinut projektin hallintaa, kuten resurssien hallintaa sekä ajan hallintaa. Tärkeää oli pilkkoa projektin vaiheet pieniin osiin ja tehdä osat valmiiksi yksi kerrallaan suunnitellussa järjestyksessä. Järjestelmällisyys oli tärkeää säilyttää loppuun asti, jotta työmäärä ei tuntunut mahdottomalta. Kesken projektin aloitin uuden kokopäivätyön, jossa myös riitti uutta opittavaa. Onnistuin suunnittelemaan resurssit riittäväksi vaikka suurin osa ajastani kuluikin kokopäivätyössä. Myös projektin suunnittelutaitoni ovat kehittyneet huomattavasti. Opin kyvyn suunnitella suurta ja pitkäkestoista projektia vaihtelevien resurssien kanssa. Opin myös kyvyn mukauttaa suunnittelua tilanteen mukaan, jos tilanne sitä vaati.

Lähteet

Aktia. Aktia Wallet. Luettavissa: https://www.aktia.fi/fi/aktia-wallet. Luettu: 13.7.2017.

Coskun, V, Ok, K & Ozdenizci B. 2011. Near Field Communication (NFC): From Theory to Practice. Wiley. Istanbul.

Dummies. The NFC Ecosystem. Luettavissa: http://www.dummies.com/consumer-electronics/the-nfc-ecosystem/. Luettu: 23.9.2017.

EasyPark. 2017. EasyPark. Luettavissa: https://easypark.fi/. Luettu: 5.6.2017.

Ecma International. Index of Ecma Standards. Luettavissa: https://www.ecma-international.org/publications/standards/Stnindex.htm. Luettu: 12.7.2017.

Haikala, N. 2016. Mobiilimaksut ovat tulleet jäädäkseen – Nordea Pay on nyt julkaistu. Luettavissa: http://mobiili.fi/2016/05/03/mobiilimaksut-ovat-tulleet-jaadakseen-nordea-pay-on-nyt-julkaistu/. Luettu: 13.7.2017.

Haikala, N. 2016. MobilePay toimii nyt myös kassoilla – ensimmäisenä mukana kesäfestarit. Luettavissa: http://mobiili.fi/2016/06/04/mobilepay-toimii-nyt-myos-kassoilla-ensimmaisena-mukana-kesafestarit/. Luettu: 13.7.2017.

Haikala, N. 2016. OP nappasi kärkisijan – lähimaksaminen puhelimella onnistuu viimein. Luettavissa: http://mobiili.fi/2016/04/06/op-nappasi-karkisijan-lahimaksaminen-puhelimella-onnistuu-viimein/. Luettu: 5.6.2017.

Hall, K. 2016. TalkTalk admits losing £60m and 101,000 customers after THAT hack. Luettavissa: https://www.theregister.co.uk/2016/02/02/talktalk_hack_cost_60m_lost_100k_customers/. Luettu: 30.9.2017.

InfoSec Institute. 2013. Near Field Communication (NFC) Technology, Vulnerabilities and Principal Attack Schema. Luettavissa: http://resources.infosecinstitute.com/near-field-communication-nfc-technology-vulnerabilities-and-principal-attack-schema/#gref. Luettu: 8.6.2017.

International Organization for Standardization. ISO/IEC 18092:2013. Luettavissa: https://www.iso.org/standard/56692.html. Luettu: 24.9.2017.

International Organization for Standardization. ISO/IEC 14443-3:2016. Luettavissa: https://www.iso.org/standard/70171.html. Luettu: 24.9.2017.

Kivioja, M. 2007. Mobiilimaksaminen lähimaksamisen näkökannalta. Tampereen ammattikorkeakoulu. Tampere.

Korttiturvallisuus.fi. Lähimaksaminen. Luettavissa: https://www.korttiturvallisuus.fi/Kaupassa/Lahimaksaminen/. Luettu: 5.6.2017.

Lainiala, P. 2016. OP otti lähimaksun käyttöön Pivo-sovelluksessa. Luettavissa: https://muropaketti.com/mobiili/mobiiliuutiset/op-otti-lahimaksun-kayttoon-pivo-sovelluksessa/. Luettu: 13.7.2017.

Marwaha, G. 2014. What is a Secure Element (SE)? Luettavissa: http://www.gmarwaha.com/blog/2014/09/01/mobile-payments-what-is-a-secure-element/. Luettu: 13.6.2017.

Mitrokotsa, A, Rieback, M & Tanenbaum, A. 2010. Classification of RFID Attacks. Luettavissa: http://www.cse.chalmers.se/~aikmitr/papers/IWRT08.pdf. Luettu: 13.6.2017.

MobilePay. Maksa nopeammin MobilePay:llä. Luettavissa: https://www.mobilepay.fi/fi-fi/Pages/mobilepay.aspx. Luettu: 13.7.2017.

NearFieldCommunication.org. Security Risks of Near Field Communication. 2017. Luettavissa: http://nearfieldcommunication.org/nfc-security-risks.html. Luettu: 27.6.2017.

NFC.cc. NFC. 2011. Luettavissa: http://www.nfc.cc/technology/nfc/. Luettu: 30.9.2017.

NFC Forum. What are the operating modes of NFC devices? Luettavissa: http://nfc-forum.org/resources/what-are-the-operating-modes-of-nfc-devices/. Luettu: 7.6.2017.

NFC World. ECMA Updates NFC Security Standards. Luettavissa: https://www.nfcworld.com/2015/08/11/337067/ecma-updates-nfc-security-standards/. Luettu: 12.7.2017.

Nordea. Nordea Pay. Luettavissa: https://www.nordea.fi/henkiloasiakkaat/paivittaiset-raha-asiat/internet-mobiili-ja-puhelinpalvelut/nordea-pay.html#tab=Ominaisuudet. Luettu: 13.7.2017.

Nets. Aktivoi lähimaksu maksupäätteeseesi tänään. Luettavissa: https://www.nets.eu/fi/payments/korttimaksut-myymalassa/lisaarvopalvelut/lahimaksaminen/. Luettu: 23.9.2017.

Osakesijoittaja.fi. Uudessa Aktia Walletissa yhdistyvät monipuolinen digitaalinen lompakko ja maksusovellus. Luettavissa: http://www.osakesijoittaja.fi/2016/10/uudessa-aktia-walletissa-yhdistyvat-monipuolinen-digitaalinen-lompakko-ja-maksusovellus/. Luettu: 13.7.2017.

Paganini, P. 2012. NFC, business opportunities, security and privacy issues. Luettavissa: http://securityaffairs.co/wordpress/5090/hacking/nfc-business-opportunities-security-and-privacy-issues.html. Luettu: 24.9.2017.

Pihkala, J. 2017. NFC-tagit. Luettavissa: http://nfc-tunniste.weebly.com/nfc-tagit.html. Luettu: 24.9.2017.

Pivo. Maksa lähimaksulla. Luettavissa: https://pivo.fi/lahimaksut/#. Luettu: 13.7.2017.

Radio-Electronics.com. NFC Security. Luettavissa: http://www.radio-electronics.com/info/wireless/nfc/nfc-near-field-communications-security.php. Luettu: 10.7.2017.

Skorobogatov, S. 2001. Semi-Invasive Attacks (definition). Luettavissa: http://www.cl.cam.ac.uk/~sps32/semi-inv_def.html. Luettu: 13.6.2017.

Söderlund, O. 2012. Mobiili lähimaksaminen tekee tuloaan Suomeen – kuka ottaa markkinan haltuunsa? Luettavissa: http://www.magentaadvisory.com/fi/2012/08/13/mobiili-lahimaksaminen-tekee-tuloaan-suomeen-kuka-ottaa-markkinan-haltuunsa/. Luettu: 5.6.2017.

Tehranipoor, M. 2012. Security for RFID Tags. Luettavissa: http://www.engr.uconn.edu/~tehrani/teaching/hst/17%20Security%20for%20RFID%20Tags.pdf. Luettu: 8.6.2017.

Triggs, R. 2017. What is NFC & how does it work? Luettavissa: http://www.androidauthority.com/what-is-nfc-270730/. Luettu: 24.9.2017.

Visa Europe. 2016. Visa Europe teki ennätyksellisen liikevaihdon viime vuonna – Suomessa jo joka neljäs euro maksetaan Visa-kortilla. Luettavissa: https://www.epressi.com/media/userfiles/4705/1455631844/visa_annual-results_fi.pdf. Luettu: 23.9.2017.

Liitteet

Liite 1 Termit ja lyhenteet

Algoritmi	Yksityiskohtainen kuvaus tai ohje siitä, miten tehtävä tai prosessi suoritetaan.
Backend	Tausta-alusta. Pohja, jonka päälle ohjelma rakennetaan.
Baudi	Tiedonsiirtonopeuden suure. Yksi baudi kuvaa elektronisen signaalin muutosnopeutta per sekunti.
Bluetooth	Avoin standardi laitteiden langattomaan kommunikointiin lähietäisyydellä.
CCD-kamera	Charge-coupled device. Valoherkkä kamera, joka muuntaa infrapunasäteilyn digitaaliseksi signaaliksi.
CMOS	Complementary metal-oxide-semiconductor. Täydentävä metallioksidi-puolijohde, joka on integroitujen piirien luokka.
ECDH	Elliptic Curves Diffie-Hellman. Diffie-Hellman avaimenvaihtojär jestelmään perustuva elliptisten käyrien salausmenetelmä.
Emulointi	Toisen koneen tai laitteen jäljitteleminen.
EPC	Electronic Product Code. Sähköinen tuotekoodi. Kansainvälisessä käytössä oleva koodi on tallennettu sähköisesti RFID-tunnisteeseen. EPC on 64- tai 96-bittinen koodi, joka on jaettu numerosarjoihin jotka sisältävät tietoa kuten valmistajan ja tuotteen tyypin.
FIB	Focused ion beam. Keskittynyt ionisäde.
Kryptograafinen	Salattu.
NFC	Near Field Communication. Radiotaajuinen etätunnistustekniikka.
NFCIP-1	NFC:n turvallisuusstandardi.
NFC-lukija	Vastaanottaa NFC-tagista saaman radiosignaalin digitaaliseen muotoon, joka välitetään edelleen älypuhelimelle tai muulle lukijalaitteelle käsiteltäväksi.
NFC-SEC	Kokoelma NFC-tietoturvastandardeja.
NFC-tagi	Mikrosirun ja antennin yhdistelmä. Antenni mahdollistaa mikrosirun tiedon välittämisen NFC-lukijalle.
PDU	Protocol data unit. Käytetty termi kuvaamaan tietoa, kun se siirtyy OSI-mallin yhdestä kerroksesta toiseen.

PID	Proportional-integral-derivative. Verrannollinen integraali-johdannainen. Valvontasilmukan takaisinkytkentämekanismi, jota käytetään laajalti teollisuusjärjestelmissä.
RFID	Radio frequency identification. Radiotaajuinen etätunnistus on menetelmä tiedon etälukuun ja -tallentamiseen käyttäen RFID-tageja.
RF-kenttä	Radio frequency field. Radiotaajuuskenttä on vaihtovirta, joka antennin kautta tuottaa sähkömagneettisen kentän langattomaan lähetykseen tai viestintään lähettämällä virran antennin läpi.
SD-kortti	Secure digital. Yleisesti älypuhelimissa käytetty muistikorttityyppi.
SE	Secure Element. Muuntamisen kestävä alusta, joka kykenee suojelemaan sovelluksia sekä niiden luottamuksellisia tietoja ja salaustietoja luotettujen tahojen sääntöjen ja turvallisuusvaatimusten mukaisesti. Tyypillisesti yhden sirun suojattu mikro-ohjain.
SIM-kortti	Subscriber identity module. Älykortti, jota käytetään matkapuhelinliittymän tilaajan yksilöllisen IMSI-avaimen tietoturvalliseen tallentamiseen.
SMS	Short message service. Tekstiviesti.
Standardi	Jonkin organisaation esittämä määritelmä siitä, miten jokin asia tulisi tehdä.
TTP	Time-triggered protocol. Avoin tietokoneverkkoprotokolla ohjausjärjestelmille. Se on suunniteltu ajallisesti käynnistetyiksi kenttäväyliksi ajoneuvoihin ja teollisiin sovelluksiin.
UICC-kortti	Universal integrated circuit card. Älykortti, jota käytetään mobiilipäätelaitteissa GSM- ja UMTS-verkoissa.
URI	Uniform resource identifier. Merkkijono, jota käytetään tunnistamaan nimi tai resurssi.
URL	Uniform resource locator. Merkkijono, jolla kerrotaan tietyn tiedon paika.
Vertaisverkko	P2P. Verkko, jossa ei ole kiinteitä palvelimia ja asiakkaita, vaan jokainen verkkoon kytketty taho toimii sekä palvelimena että asiakkaana verkon muille jäsenille.
Wi-Fi	WLAN. Wireless local area network. Langaton lähiverkkotekniikka, jolla erilaiset verkkolaitteet voidaan yhdistää ilman kaapeleita.

Viitekehys	Tarkoituksena on tavoittaa tutkittavassa ilmiössä keskeiset tekijät ja niiden väliset suhteet.
VLSI	Very-large-scale integration. Prosessi luoda integroitu piiri yhdistämällä tuhansia transistoreja yhdeksi siruksi.
Väliohjelmisto	Ohjelmisto, joka toimii siltana käyttöjärjestelmän tai tietokannan ja sovellusten välillä erityisesti verkossa.
Älykortti	Muovinen kortti, johon on upotettu mikropiiri.

Liite 2 Kysely

Tällä kyselyllä kartoitetaan lähimaksupalveluiden käyttöä. Kysely on osana Opinnäytetyötä, jossa tutkitaan lähimaksupalveluiden turvallisuutta. Kyselyyn vastaaminen vie pari minuuttia ja vastaukset käsitellään anonyymisti. Kiitos ajastasi.

1. Kuinka turvallista lähimaksaminen mielestäsi on?
Jos et ole käyttänyt lähimaksuominaisuutta jätä vastaamatta kysymykset 1-3 ja aloita vastaaminen kysymyksestä 4.

- ○ Erittäin turvallista
- ○ Melko turvallista
- ○ Hieman vaarallista
- ○ Erittäin vaarallista
- ○ En osaa sanoa

2. Minkä takia pidät lähimaksamista vaarallisena?

- ☐ Lähimaksukortin tai -laitteen joutuminen varastetuksi
- ☐ Lähimaksulukijan joutuminen varastetuksi
- ☐ Salakuuntelu (Tiedon sieppaaminen lähimaksukortista tai -laitteesta)
- ☐ Maksuohjelmiston tietoturvapuutteet
- ☐ Pidän lähimaksamista turvallisena
- ☐ En osaa sanoa
- ☐ Muu, mikä? _____

3. Minkä takia pidät lähimaksamista turvallisena?

- ○ En osaa sanoa
- ○ Pidän lähimaksamista turvallisena, koska _____

4. Mitä lähimaksumuotoja käytät? *

- [ ] Pankkikortin lähimaksuominaisuus
- [ ] Pivo
- [ ] Nordea Pay
- [ ] Aktia Wallet
- [ ] MobilePay
- [ ] En käytä
- [ ] Muu, mikä? _____

5. Kuinka kauan olet käyttänyt lähimaksuominaisuutta? *

- ○ Alle 6 kuukautta
- ○ 6-12 kuukautta
- ○ 12-18 kuukautta
- ○ 18-24 kuukautta
- ○ En ole käyttänyt
- ○ Muu, mikä? (kuukautta) _____

6. Kuinka usein käytät lähimaksuominaisuutta?
Jos et ole käyttänyt jätä vastaamatta.

- ○ Kerran päivässä
- ○ 1-6 kertaa viikossa
- ○ 1-3 kertaa kuussa
- ○ Useita kertoja päivässä, monta? _____

7. Missä käytät lähimaksuominaisuutta? *

- [ ] Päivittäistavarakaupat
- [ ] Kioskit
- [ ] Tavaratalot
- [ ] Ravintolat
- [ ] Festivaalit/Tapahtumat
- [ ] Yökerhot/Pubit
- [ ] Automaatit/Itsepalvelupisteet
- [ ] Kulkuvälineet
- [ ] En missään
- [ ] Muu, mikä?

Palauta kysely